

FRONTIER MARKETS PTY LIMITED

ANTI MONEY LAUNDERING AND KNOW YOUR CLIENTS POLICY

Applicability and objectives

This Policy sets out the control standards and procedures that should exist in FRONTIER MARKETS (PTY) LTD ("We", "Company") or the "Firm") in relation to Anti Money Laundering. The overall aim is to provide a comprehensive analysis of the policies and procedures applied by FRONTIER MARKETS Pty Ltd to counterfeit money laundering and terrorist financing.

Approved by:	Name:	Position:	Date:
Policy Owner	FRONTIER MARKETS Pty Ltd Name: Fransoa Daniel Swart	CEO	01.03.2024

Version no:	Date:	Author:	Main changes (if any):
1	01.03.2024	Fransoa Daniel Swart	n/a

Contents

1.	PURPOSE	4
2.	LEGAL FRAMEWORK	5
3.	ROLES AND RESPONSIBILITIES	6
3.1	Board of Directors Obligations	6
3.2	Internal Auditor's Obligations	7
3.3	MLRO's Obligations	7
3.4	Duties of MLRO	12
3.5	Duties of the Company's Employees	12
3.6	Reporting lines	12
4.	CLIENT ACCEPTANCE POLICY	13
4.1	Risk Based Approach in client verification	13
4.2	Acceptance of deposits and trading	17
4.3	Inability to complete CDD	19
4.4	Simplified client due diligence – Low risk clients	19
4.5	Enhanced client due diligence – High risk clients	21
4.6	Standard Client due diligence- Medium Risk Clients	22
4.7	Approval of clients	22
5.	CLIENT'S ECONOMIC PROFILE	22
6.	CLIENT IDENTIFICATION – Additional Guidance	24
6.1	Identification of Ultimate Beneficial Owners (UBOs)	24
6.2	Politically Exposed Persons (PEP)	24
6.3	Joint accounts	27
6.4	Anonymous or Numbered accounts	27
6.5	non-Acceptable clients	28
6.6	Lead and Practice Account	28
6.7	Deceased client	28
6.8	Underage clients	29
6.9	Reliance on third parties for KYC identification	30
7.	DOCUMENTATION	30
7.1	Documentation standards	30
7.2	Supporting documentation:	31
7.3	Document verification	32
7.4	Reliable/ independent authenticators for document certifications	32
7.5	Language of documentation	33
8.	ELECTRONIC VERIFICATION	33

9.	AML/KYC MONITORING PROCEDURES	34
9.1	Updating clients' files	34
9.2	Ongoing monitoring of clients trading activity	35
9.3	Funds transfers (Deposits & Withdrawals)	36
10	APPROVAL OF BUSINESS INTRODUCERS, AFFILIATES AND BUSINESS TO BUSINESS	38
10.1	Approval process for Business Introdurers and Affiliates	39
10.2	Business to Business ("B2B") activities and approval process	41
11	REPORTING OBLIGATIONS TO FIC-	42
11.1	Recognition of suspicious transactions	42
11.2	Reporting of suspicious transactions to FIC-	43
12	RECORD KEEPING	44
13	TRAINING	46
	APPENDIX 1: Internal Suspicion Report	48
	APPENDIX 2: Internal Evaluation Report	49
	APPENDIX 3: EU equivalent jurisdictions	50
	APPENDIX 4: High-Risk Clients	51
	APPENDIX 5: Joint Account Application Forms	53
	APPENDIX 6: FATF High-Risk and Non-cooperative jurisdictions	55
	APPENDIX 7: Client Identification Checklist	57
	APPENDIX 8: Joint Bank Account Declaration Form	61
	APPENDIX 9: Declaration of Cash Deposits	62
	APPENDIX 10: Investigation Form	66
	APPENDIX 11: AML Questionnaire	68
	APPENDIX 12: Suspicious Transactions	71
	APPENDIX 13: Offences that relate to proceeds of unlawful activity	71
	APPENDIX 14: FICA Guidance Note	71

1. PURPOSE

The purpose of this Anti Money Laundering (AML) and Know Your Clients (KYC) Policy (Collectively referred to as Policy) is to set out the principles and procedures employed by FRONTIER MARKETS (PTY) LTD (the Company) in relation to the:

- prevention and suppression of money laundering and terrorist financing.
- implementation of a risk-based approach in identifying clients, their sources of funds and client classification to minimize operational and reputation risks; and
- achieving full compliance with the relevant anti money laundering laws and regulations.

In addition, this Policy is intended to:

- bring awareness to the Company's personnel of their reporting and other obligations in relation to activities which raise suspicions of money laundering activity and/or financing of terrorism; and to
- Prescribe the role of the Money Laundering Reporting Officer (MLRO) and his/her obligation to report suspicious activity to the Financial Intelligence Centre (FIC) established in terms of The Financial Intelligence Centre Amendment Act, 2008 (the Amendment Act).

This document applies to all the Company's personnel and should be read in conjunction with other related policies. Where any provisions are in conflict, this document should take precedence. It is clarified that this document is not intended to cover all eventualities and all circumstances that may be encountered on a day-to-day basis. Where such circumstances arise, input from the MLRO shall be provided as appropriate.

The person responsible for monitoring compliance of FRONTIER MARKETS (PTY) LTD is "Outsourced Compliance" (External Compliance Officer).

2. CURRENT LEGAL POSITION AND PENALTIES

Money laundering in South Africa is currently regulated by:

- Prevention of Organised Crime Act No, 1998 (POCA).
 - a) This is a South African piece of legislation which creates the main money laundering offenses and provides for the forfeiture of the proceeds of crime. POCA came into force on 21 January 1999.
 - b) POCA criminalized money laundering in three separate provisions which cover the conversion of, transfer, concealment or disguise, possession, or acquisition of property in a manner that is largely consistent with the 1998 United Nations (UN) Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) and the 2000 UN Convention against Transactional Organised Crime (Palermo Convention).
- FICA: Different sections came into force on different dates (chapter 1: sections 1-16; chapter 2: sections 17-20 and chapter 4: sections 72-82 (except section 79) came into operation on 1 February 2002. Chapter 3 and section 79 came into force on 30 June 2003).
- The Regulations promulgated in terms of FICA and POCA.
- Protection of Constitutional Democracy against Terrorist and Related Activities Act No, 2004 (POCDATARA). This is a South African piece of legislation that imposes the duty to report any terrorist or terrorist related acts.

(Collectively referred to as the AML Legislation).

Salient Definitions and Requirements

- Both FICA and POCA are in keeping with global trends aimed at curbing the proceeds of crime, money laundering and the funding of terrorism. POCA is an omnibus Act dealing, among other things, with money laundering, racketeering and criminal and civil forfeiture. FICA creates the FIC and contains reporting and KYC obligations. POCA and FICA apply to "*proceeds of unlawful activities*" which is defined as:

"Any property or any service, advantage, benefit, or reward which was derived, received, or retained, directly or indirectly, in South Africa or elsewhere, at any time before or after the commencement of POCA, regarding or because of any unlawful activity carried on by any person, and includes any property representing property so derived"

"Property" means "*money or any other movable, immovable, corporeal or incorporeal thing and includes any rights, privileges, claims and securities and any interest therein and all proceeds thereof*".

"Unlawful activity" means "*conduct which constitutes a crime, or which contravenes any law, whether such conduct occurred before or after the commencement of POCA and whether such conduct occurred in the Republic or elsewhere*".

- POCA sets out the substantive money laundering offences. In South Africa the acquisition, possession, or use of proceeds of unlawful activities does not apply to the person who committed the predicate offence. South Africa adapts an "*all crimes*" approach which covers a range of offences in each of the 20 designated categories of offences. There is also a broad range of ancillary offences to the money laundering offences. In broad outline, these offences are the money laundering offence itself, assisting another to launder the proceeds of unlawful activity, and the acquisition, use or possession of laundered property. In view of the import of these provisions, and for ease of reference, these provisions are set out in Appendix 13.
- FICA complements POCA and provides an administrative framework to combat money laundering. In terms of FICA, rigorous compliance obligations are imposed on accountable institutions, of which the Company is one. Accountable institutions are obliged to:
 - identify and verify new and existing clients
 - keep records of identities of clients and of transactions entered with clients
 - report certain transactions to FIC.
 - formulate and implement internal rules.
 - train employees; and
 - appoint a responsible person to monitor compliance.
- South Africa criminalised terrorist financing in Section 4 of the POCDATARA, which is a comprehensive Act that criminalises the collection or provision of property with the intention that it be used for committing a terrorist act by a terrorist organisation or individual terrorist for any purpose. The term "property" is broadly defined and there is no requirement that the property, be used to carry out and or attempt a terrorist act or be linked to a specific terrorist act. Terrorist financing is also a predicate offence for money laundering. The purpose of this Policy is not to go into detail on the criminal and civil

forfeiture regime that exists. As an employee you are, however, expected to know how to deal with a client that has committed or has been suspected of committing the predicate offences.

- The **money laundering** offences are, in summary:

- o A person is guilty of money laundering if knowing or believing that property is or represents the proceeds of criminal conduct, or being reckless as to whether it is or represents the proceeds of criminal conduct:
 - i. he converts, transfers, or handles the property or removes it from the Republic of South Africa with the intention of concealing or disguising the nature of the property and its ownership, or assists another person to avoid prosecution or the making or enforcement of a confiscation order; or
 - ii. he conceals or disguises the true nature, source, location, disposition, movement or ownership of the property or any rights with respect to it; or
 - iii. he acquires, possesses, or uses the property.

*A person is to be regarded as acting knowingly or recklessly if the surrounding circumstances are such that it is reasonable to conclude that to be the case unless the individual concerned can provide proof of legal authority or excuse for his or her actions.

*Believing property to be, or represent, another person's criminal proceeds, includes thinking that the property was probably, or probably represented, proceeds of criminal conduct.

- o It is an offence for a designated body to fail to maintain the records required by FICA or to fail to adopt measures to prevent and detect money laundering.
- o It is an offence for a designated body, its directors, employees, and officers to fail to make a report as required by the FICA.
- o The act of tipping off is an offence under the Act. This may occur where a person who, knowing or suspecting that an investigation is taking place, makes any disclosure likely to prejudice the investigation arising from a report under the Act.
- o There are, however, two stated defences that a person may rely on.
 - i. that he did not know or suspect that the disclosure to which the proceedings relate was likely to prejudice the investigation; and
 - ii. that he had lawful authority or reasonable excuse for making the disclosure.
- o It is not necessary that the original activity from which the proceeds stem was committed in South Africa.
- o There is no obligation on a financial institution to enquire into the specific criminal offence underlying the suspicious transaction.

- The **Financing Terrorism** offences are, in summary:

- o A person is guilty of financing terrorism if they, in or outside South Africa, directly or indirectly, unlawfully and wilfully, provide, collect or receive funds intending that they be used or knowing that they will be used to carry out an act that is an offence under South African law, or that is within the scope of and defined in any treaty listed in the Terrorist Financing Convention, or any other act that is intended to cause death or serious bodily injury to a civilian or other person not taking part in an armed conflict, the purpose of which is to intimidate a population or to compel a government or an international organisation to do, or abstain from doing, any act; or if they attempt to commit the offence.

- o It is also an offence to directly or indirectly, unlawfully, and wilfully provide, collect or receive funds intending that they be used or knowing that they will be used for the benefit or purposes of a terrorist group.
- Penalties relevant to the administration of the Policy

In terms of Section 68(2) of FICA, a person convicted for failure to provide training or appoint a Compliance Office; tipping off; failure to report; failure to adopt and implement rules; failure to register with FIC and offences relating to inspection and non-compliance with court processes will be liable to imprisonment for a period not exceeding 5 years or to a fine not exceeding R10 million.

3. ROLES AND RESPONSIBILITIES

The Company must ensure that the governing body defines, oversees and is accountable for the implementation of corporate governance arrangements that ensure effective and prudent management of the Company.

3.1 Board of Directors Obligations

The Board of Directors' (Board's) overriding principle is that the Company should be compliant with applicable AML Legislation. As part of its overall responsibility, the Boards' obligations are to:

- determine, record, and approve the general policy principles of the Company in relation to the prevention of money laundering and terrorist financing and communicate them to the Money Laundering Reporting Officer (MLRO).
- appoint a compliance officer and, where necessary, assistant compliance officers and determine their duties and responsibilities, which are recorded in the relevant section of this Policy.
- approve this Policy, which is communicated to all employees of the Company that manage, monitor, or control in any way the customers' transactions and that have the responsibility for the application of the practices, measures, procedures, and controls that have been determined.
- ensure that all requirements of the Law are applied, and that appropriate, effective, and sufficient systems and controls are introduced for achieving the abovementioned requirement.
- assure that the MLRO and his assistants (if any) and any other person who has been assigned with the duty of implementing the procedures for the prevention of money laundering and terrorist financing, have complete and timely access to all data and information concerning customers' identity, transactions documents and other relevant files and information maintained by the Company to be fully facilitated in the effective execution of their duties.
- ensure that all employees are aware of the person who has been assigned with the duties of the MLRO and his assistants, to whom they report any information concerning transactions and activities that they suspect might be related to money laundering and terrorist financing.
- establish a clear and quick reporting chain in terms of which suspicious transactions must be passed without delay to the MLRO, either directly or through his assistants.
- ensure that the compliance officer has sufficient resources, including competent staff and technological equipment, for the effective discharge of his duties.

- assess and approve the annual report of the MLRO and to take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the annual report.
- communicate to the MLRO the AML related guidelines; and
- review and approve the AML training plan which is submitted by the MLRO.

3.2 Internal Auditor's Obligations

The internal auditor's obligations in relation to this Policy are to:

- review and evaluate, at least on an annual basis, the appropriateness, effectiveness and adequacy of this Policy and the practices, measures, procedures, and control mechanisms applied for the prevention of money laundering and terrorist financing. The exact program to be followed is outlined in the annual internal audit plan which is provided by the internal auditor at the beginning of each year.
- ascertain the integrity and reliability of financial and other information provided to the Board, including that which is used in decision making.
- ascertain those systems of control are laid down and operate to promote the economic, efficient, and effective use of resources.
- submit the findings and observations, in the form of a written report, to the Board which decides the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected; and

The minutes of the abovementioned decisions of the Board and the internal auditor's report must be kept on file by the Company and the internal auditors.

3.3 MLRO's Obligations

- The MLRO's obligations in relation to this Policy are to:
 - a) design the internal practice, measures, procedures, and controls relevant to the prevention of money laundering and terrorist financing and to describe and allocate the appropriateness and the limits of responsibility of each department that is involved.
 - b) develop and establish the customers' acceptance policy and to submit it to the Board for consideration and approval.
 - c) prepare a risk management and procedures manual regarding money laundering and terrorist financing.
 - d) monitor and assess the correct and effective implementation of this Policy.
 - e) receive information from the employees which is knowledge or suspicion of money laundering or terrorist financing activities, or which might be related to such activities. The information is received through the "Internal Suspicion Report" which is included as **Appendix 1** of this Policy.
 - f) evaluate and examine the information received as per point (e). The evaluation of the information is being done in the form of a report, referred to as the "Internal Evaluation Report". An example is included as **Appendix 2** of this Policy, however, the MLRO may use a different form as he deems appropriate.
 - g) notify FIC of any suspicion through the goAML online system. provide guidance to the employees on subjects related to money laundering and terrorist financing.
 - h) prepare a "Monthly Prevention Statement" for the prevention of money laundering and terrorist financing, which must be readily available on request by the FSB and FIC.
 - i) prepare the MLRO's annual report.

- j) maintain a registry which includes the reports of points (e), (f) and (g), and relevant statistical information (department that submitted the internal report, date of submission to the compliance officer, date of assessment, date of reporting to FIC), the evaluation reports of point (d) and all the documents that verify the accomplishment of his duties specified in the present subparagraph.
- k) maintain a list of clients who are categorized following a risk-based approach, which contains, *inter alia*, the names of clients, their account numbers, and the dates of the commencement of the business relationships. Moreover, the MLRO ensures the updating of the said lists with all new or existing clients, in the light of additional information obtained.
- l) review, on an annual basis, the appropriateness of policies and procedures, given to new clients, geographical areas of operations and new financial instruments and to implement corrections. Particular attention is to be given to electronic/internet trading and telephone orders.
- m) evaluate the systems and procedures applied by a third person on whom the Company relies for client identification and due diligence procedures, and to approve the cooperation with it.
- n) provide advice and guidance to the Company's personnel on subjects related to money laundering and terrorist financing.
- o) assess the training needs of the Company's departments and employees. The MLRO will prepare and apply annual staff training programs and will further record the seminars/training courses attended by each employee; and
- p) reply to all requests and queries from FIC and the FSB.

- Annual report of the MLRO

- a) The Annual MLRO's Report (AML Report) is prepared by the MLRO and submitted to the Board for discussion and approval, at the latest by end of February following the year under review.
- b) The content of the AML Report shall include, at a minimum, the following:
 - i. information about measures undertaken and/or procedures introduced by the Company for compliance with any amendments and/or new provisions of the AML Legislation which took place during the year under review.
 - ii. reference to changes or upcoming changes (if already known) of the regulatory framework regarding the prevention of money laundering and terrorist financing, such as legislation and relevant regulations and circulars.
 - b. reference to relevant data, information, and reports from international organizations.
 - c. specific measures and procedures taken/adopted concerning the above.
 - d. suggestions for further measures and implementation of further procedures in the case of any weaknesses or deficiencies in relation to points i and ii above, setting a timeframe for implementation.
 - e. information on the reviews performed by the MLRO during the year, reporting material weaknesses and deficiencies identified in the policy, practices, measures, procedures, and controls that the Company applies for the prevention of money laundering and terrorist financing. In this respect, the report outlines the seriousness of the deficiencies and/or weaknesses identified, the risk implications and actions taken and/or recommendations made for rectifying the situation.
 - f. specific reference to the content and the method/way of conducting of the inspections and reviews, regarding at least the following sectors:
 - ✓ completeness of the AML manual.
 - ✓ implementation of customers' acceptance policy.
 - ✓ constructions and content of economic profile.
 - ✓ identification of suspicious transactions, internal suspicion reporting and external reporting to FIC.
 - ✓ simplified customer identification and due diligence procedures of low-risk customers.

- ✓ customer identification and due diligence measures of normal risk customers.
 - ✓ enhanced customer identification and due diligence procedures of high-risk customers.
 - ✓ timing of customers' identification.
 - ✓ reliance on third parties for customer identification and due diligence purposes.
 - ✓ ongoing monitoring of customers' accounts and transactions.
 - ✓ record keeping.
 - ✓ implementation of measures and procedures on a risk-based approach.
 - ✓ implementation of the financial sanctions as required by AML legislation and the FIC from time to time.
 - ✓ measures and procedures taken for the compliance of branches and subsidiaries of the Company, the (Regulated Entity"), operating in countries outside South Africa; and
 - ✓ education and training of staff.
- g. specific reference to the content and the method/way of conducting of the inspections and reviews, regarding at least the following sectors: -
- ✓ the number of Internal Suspicion Reports submitted to the MLRO by the Company's employees and possible comments/observations thereon.
 - ✓ the number of Internal Suspicion Reports submitted by the employees of the regulated entity to the Compliance Officer and MLRO and comparative data with the previous year.
 - ✓ the number of Internal Suspicion Reports that have not been notified to FIC and comparative data with the previous year.
 - ✓ circumstances that led to the increase/decrease of Internal Suspicion Reports and significant trends observed.
 - ✓ the number of reports submitted by the MLRO to FIC with information/details on the main reasons for suspicion and highlights of any trends such as.
 - ✓ information on cases related to money laundering and terrorist financing for which no report was made.
 - ✓ the number of Compliance Officer's Reports together with the comparative date with the previous year; and
 - ✓ a summary of data/information for the main reasons of the suspicion and significant trends observed.
 - ✓ feedback from FIC regarding the submitted reports, if any.
- h. summary figures, on an annualized basis, of clients' total cash deposits in Rands and other currencies in excess of the set limit of R25,000 (together with comparative figures of the previous year) as reported in the Monthly Prevention Statement.
- i. any comments on material changes observed compared with the previous year are also reported.
- j. reference on an annual basis of customers' total cash deposits, in Rand and other currencies in excess of the set limit of R25.000 reported in the Monthly Prevention Statement and comparative data with the previous year.
- k. circumstances that led to the increase of customers' cash deposits and significant trends observed.
- l. reference to the measures and actions of the regulated entity regarding cash deposits by customers (e.g., method/way of identification and investigation, recording the investigation in the customer's file, result of the investigation and possible actions taken).
- m. recommendations for further actions and implementation of further procedures in case of deficiencies and weaknesses in relation to the point above, setting a timeframe for implementation.
- n. information, details, or observations regarding the communication with the employees on money laundering and terrorist financing preventive issues.

- o. information on the policy, measures, practices, procedures, and controls applied by the Company in relation to high-risk clients as well as the number and country of origin of high-risk clients with whom a business relationship is established or an occasional transaction has been executed.
- p. information on this Policy, measures, practices, procedures, and controls applied by the regulated entity in relation to high-risk customers.
- q. number, country of origin and type of high-risk customers with whom a business relationship is established, or an occasional transaction has been executed and comparative data with the previous year.
- r. information about systems and procedures applied by the Company for the ongoing monitoring of client accounts and transactions.
- s. analysis of the way/method (automated or non-automated) of the ongoing monitoring of customers' accounts and transactions.
- t. details for any variation of the ongoing monitoring of customers' accounts and transactions according to the customer's categorization on a risk-based approach.
- u. details of the timing of the ongoing monitoring of customers' accounts and transactions (e.g., in real time or after the completion of an event).
- v. details of the way/method of documenting the ongoing monitoring of customers' accounts and transaction.
- w. information on training courses attended by the MLRO and any other educational material received.
- x. information on training/education and any educational material provided to staff during the year; reporting, the number of courses/seminars organised, their duration, the number and the position of the employees attending, the names and qualifications of the instructors, and specifying whether the courses/seminars were developed in-house or by an external organisation or consultants
- y. reference to specific issues/cases, questions/clarifications, and any other form of communication with the staff and the specific results that have arisen from the relevant communication.
- z. information on training courses/seminars attended by the Compliance Officer and the rest of the staff of the Company during the year **and** for the next year which will include:
 - ✓ summarized data of the program/content of the training courses/seminars.
 - ✓ number and duration of the training courses/seminars.
 - ✓ number and position of the employees participating in the training courses/seminars.
 - ✓ number and position of employees who did not participate in the training courses/seminars and their duties are relevant with the prevention of money laundering and terrorist financing and information on the reasons for not participating.
 - ✓ instructors' names and qualifications.
 - ✓ whether the training courses/seminars were performed in-house or by an external organization or consultants; and
 - ✓ information for the educational material received.
 - ✓ results of the assessment of the adequacy and effectiveness of staff training.
 - ✓ information on the recommended next year's training program; and
- aa. information on the structure and staffing of the department of the MLRO as well as recommendations and timeframes for their implementation and information in respect of the additional staff and technical resources which may be needed for reinforcing the measures and procedures against money laundering and terrorist financing.

- Monthly Prevention Statement

The Monthly Prevention Statement includes details for the total cash deposits over R25,000 or equivalent amount in other currency accepted by the Company, the Internal Suspicious Activity/Transactions Report and the MLRO's reports to FIC. The completion of the said report offers the opportunity to evaluate and reinforce the Company's systems of controls and monitor the Company's operations in respect of early identification and detection of cash transactions which increase the risk of money laundering and terrorist financing activities taking place.

- Right of Access

The MLRO, as well as any assistants/associates that he may utilize to this end have, through relevant organizational arrangements, full and prompt access to all client data, including indicative data on clients' identities and clients' transactions.

The MLRO has a professional obligation to report, directly to the Board, any incidents where his work was interrupted and/or inhibited by any person within the internal organization.

3.4 Duties of MLRO

The MLRO reviews and assesses on a bi-annual basis, the AML and KYC procedures that are followed by the Company. In addition, the MLRO approves any changes that may occur in this Policy.

3.5 Duties of the Company's Employees

- The Company expects its employees to perform the following:
 - a) conduct business in accordance with applicable AML Legislation, corporate policies, and the highest ethical standards.
 - b) do not provide advice or other assistance to persons who attempt to violate or avoid anti-money laundering laws or corporate policies.
 - c) consider the MLRO's approval or rejection of any disputable transaction as final and binding.
 - d) fully execute their obligations against the law and to disclose any suspicions about a transaction that might be related to money laundering and terrorist financing.
 - e) adequately record and retain details of all transactions undertaken with or for third parties, including payments and receipts of funds, as well as all dealings in financial instruments. At all times, the policy for third party deposits must be adhered to.
 - f) that they do not tipoff a client by notifying them of their suspicion or the fact that an employee has made a report; and
 - g) where the employee begins to suspect that a money laundering activity is taking place, even if he has already assisted the suspected launderer, he must immediately report the matter to the MLRO. The communication to the MLRO should be in the form of a written report referred to as an 'Internal Suspicion Report' (see **Appendix 1** of this Policy). Failure to do so is itself a criminal offense in the Republic of South Africa. The MLRO will advise on how to proceed in subsequent dealings with the client.

- The Company's employees who fail to fulfil their obligations or adhere to the provisions in this Policy and AML Legislation shall face internal disciplinary actions, as may be decided by their direct supervisor, the MLRO and the CEO of the Company, including termination of their employment agreement.

3.6 Reporting lines

- The following reporting lines have been set by the Company:
 - a) MLRO reports to senior management and members of the Board.
 - b) The assistants of the MLRO report to the MLRO; and
 - c) employees of customer support/back office/finance report to the MLRO where needed.

4. CLIENT ACCEPTANCE POLICY

4.1 Risk Based Approach in client verification

The Company applies appropriate measures and procedures, using a risk-based approach, to focus its effort on those areas where the risk of money laundering and terrorist financing appears to be higher. A risk-based approach is adopted by the Company during the verification of the clients', the collection of information for the construction of their economic profile and monitoring of their transactions and activities. Taking into consideration the assessed risk, the Company determines the type and extent of measures it should adopt to manage and mitigate the identified risks.

The client acceptance procedure is prepared following detailed assessments of the risks faced by the Company from its clients and/or their transactions and/or their countries of origin or operations and/or any other factors the Company may identify as significant from time to time. The Company identifies its client's prior or during the commencement of a business relationship and demonstrates that the KYC process has been completed in line with the AML Legislation prior to or during the commencement of such relationship.

Due diligence procedures are applied in the following cases:

- a) when establishing a business relationship.
- b) when carrying out once-off transactions amounting to R50,000.00 (Fifty thousand rand) or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked.
- c) when there is a suspicion of money laundering or terrorist financing, irrespective of the amount of the transaction; and
- d) when there are doubts about the veracity or adequacy of previously obtained client identification data.

The Company conducts the verification of the identity of the customer and the beneficial owner during the establishment of the business relationship since this is necessary in order not to interrupt the normal conduct of business when the money laundering and terrorist financing risk is low. The verification of clients' information is made in two ways, via the submission of documents or electronically.

4.1.1 Timing of client identification

The Company identifies the client prior to the establishment of the business relationship and proceeds with verification of the potential client's identity prior or during the establishment of a business relationship if not to interrupt the normal conduct of business and where there is limited risk of money laundering or terrorist financing occurring. In case of the latter, the due diligence procedure shall be completed as soon as practicable after the initial contact. The said procedure is further elaborated under section 4.2.2 below. Where the risk of money laundering and terrorist financing cannot be determined as low the CDD (Client Due Diligence) must be completed prior the establishment of a business relationship. Each account holder is required to complete the CDD by submitting the relevant KYC documentation or pass electronic verification.

If a client/investor, declines to cooperate the matter must be reported to the MLRO, who will decide whether to continue with the transaction or what other steps to take.

No funds should be transferred for the benefit of an identification subject until the identification process is complete.

4.1.2 Client acceptance policy and risk classification

The establishment of a business relationship is considered by the Company to commence upon the client being marked as "Compliant" in the Company's Customer Relationship Management system, namely (CRMBO) and/or when the client can trade on a real account with his/her own funds, in which case the natural or legal person is accepted by the Company as a client.

In terms of the Financial Action Task Force (FATF) guidelines, the Company will incorporate a risk-based approach to identifying its clients. The client acceptance policy is determined and implemented under criteria related to the client's risk profile. In particular, the factors that specify the risk category of a client are the following:

- a) type of client (natural or legal person).
- b) nature of business.
- c) country of domiciliation/ residency, especially if from high-risk countries or from countries known for high-level of corruption or organized crime or drug trafficking (e.g., a client is listed on the United Nations List).
- d) information used to construct the economic profile.
- e) amount of deposited funds (for subsequent re-classification after acceptance).
- f) trading Activity (for subsequent re-classification after acceptance).
- g) potential involvement of politically exposed persons ('PEPs').
- h) willingness to provide documentation.
- i) product type.
- j) duration of client's relationship with the Company; and the
- k) source of funds.

During the on-boarding process, on client completing the registration process (in the case of natural persons- online completion, in the case of legal persons- completion of hard-copy), an account is created and allocated to the client. The AML risk classification is also assigned to the client at this point following the construction of the client's economic profile.

Despite proper completion of the account registration by a potential client, he is not considered as accepted until verification of the due diligence process, following which the client will be permitted to commence trading. It is noted that the client will **not be** able to use the deposited funds until he has provided the necessary supportive information/documentation for the Company and has complied with the Company's policies for verification of the ownership of the payment method.

Based on the aforementioned and given the nature of the Company’s business being conducted through its online trading websites rather than physical interaction, most of the clients of the Company are considered non-face-to-face, therefore by default are categorized as High-Risk clients. Enhanced customer identification and due diligence measures are in place to effectively mitigate the risks associated with such business relationships as prescribed below.

The main client types and the indicative AML risk status assigned to each type, are outlined in TABLE 1 below. It is clarified that it is in the discretion of the MLRO to reclassify a client to a higher or lower risk category where there are circumstances he/she deems appropriate justifying such reclassification.

	Client Type	AML Risk Category
1	Credit or financial institutions regulated in EU or EU equivalent jurisdictions acting as principals.	Low-Risk
2	Public companies listed in EU markets or EU equivalent jurisdictions.	Low-Risk
3	Domestic public authorities in EU.	Low-Risk
4	Credit or financial institutions regulated in non-EU or Non-EU equivalent jurisdictions acting as principals	Medium Risk
5	Public companies listed in non-EU markets or non-EU equivalent jurisdictions.	Medium Risk
6	Unregulated private companies irrespective of jurisdiction.	High-Risk
7	Private companies owned by PEPs.	High-Risk
8	Companies whose shares are in bearer form.	High-Risk
9	Trusts.	High-Risk
10	'Client accounts' in the name of a third person.	High-Risk

11	Non-face to face Individuals/ Natural persons	High-Risk
12	Politically Exposed Persons.	High-Risk
13	Customer offering electronic gambling/gaming through the internet.	High-Risk
14	Customers from countries which inadequately apply Financial Action Task Force's recommendations.	High-Risk

The Company may at any given time, and following consultation with the MLRO, decide not to accept specific types of natural or legal persons as clients. The Company as at the date of this policy does not accept the following types:

1. Client accounts in the name of a third person.
2. Companies whose shares are in bearer form.
3. Customers from countries which inadequately apply FATF's recommendations
4. Trusts.

Clients on boarded through non-face to face interaction are classified as High-Risk. Given the nature of the Company's activities where all clients are non-face to face, registering on the Company's trading platforms, the Company has proceeded to introduce three subcategories within the High-Risk classification. This enables the Company to deploy its AML efforts on a more granular risk-based approach. These three subcategories in the High-Risk classification are as follows:

- **High-High Risk Client.**
- **High-Medium Risk Client; and**
- **High-Low Risk Client.**

Legal entities and Joint accounts are considered by the Company to be of higher risk and are therefore, classified as of High-Medium risk. PEPs are considered of higher risk and are classified as High-High.

Following an assessment of the customer's profile following initial registration, based on the customer's risk-scoring and subsequent monitoring, reclassification may follow, and a client may be subjected to additional requirements in accordance with the risk-based approach followed by the Company.

As mentioned above, the client's AML risk classification is always assigned prior to the commencement of the business relationship as part of the client's Compliance approval process and is recorded in the CRMBO.

4.2 Acceptance of deposits and trading

- 4.2.1 Trading during the establishment of a business relationship: The Company only enables a client to trade during the establishment of the business relationship when the customer is deemed as being of low risk of money laundering and terrorism financing. Clients who are unable to provide a Proof of Identity (POI) and Proof of Residence (POR) are not on boarded. Clients are only permitted to trade upon satisfying the established due diligence requirements.
- 4.2.2 Demo/Practice accounts trading: In the case of practice/demo accounts, the Company permits trading without requesting the demo client to complete the CDD process, since such accounts do not carry any risk of money laundering as the trading is on a virtual environment with virtual funds. Trading on demo accounts enables a client and/or potential client to familiarize himself with a near-real trading environment. Nonetheless, when a client proceeds with the transfer from a demo to a real trading account, the Company must complete CDD measures as these are analyzed below.
- 4.2.3 Trading on real platform with virtual funds (e.g., bonus): In addition to the above, the Company may also permit trading on the real platform in situations where the client and/or potential client has not completed the CDD and has made (or not made) a deposit but he is using funds credited by the Company as a bonus and/or award prior to the client making any deposits. Such funds in the aforementioned situation are considered as **virtual** which the client may not withdraw regardless of volume prior to the completion of the CDD procedure (i.e., submission of full KYC documents). The aforementioned scenario may also give the tools to a client to acquire sufficient knowledge and experience in a real platform under real market conditions without facing the risk of loss of funds and does not involve any risks of money laundering. In this situation, the client is not able to trade with real funds on the real trading platform prior to completing the CDD procedure.

It should be clear that in situations where an account has been created but problems of verification arise during the establishment of the relationship that cannot be resolved (such as provision of fake documents, identification of minor customers, etc), the Company closes or blocks access to the account.

4.3 Inability to complete CDD

In the case where a client/potential client is unable to comply with the CDD requirements, the Company may proceed with one of the following measures, on a case-by-case basis:

- i. not proceed with the establishment of the business relationship.

- ii. not proceed with execution of requested transaction by the client.
- iii. The Company must:
 - a. Return the funds as part of the termination process and close the account. In this case, the relationship is to be considered void and the funds must be returned to a bank account in the name of the depositor.
 - b. Where the Company is unable to return the funds to its source of deposit, it must retain the funds in a separate bank account until the client completes the CDD procedure to the Company's satisfaction to be able to withdraw the funds. Such deposits must be reported to the MLRO to assess whether it is justified under the circumstances to submit a report to FIC, in which case the Company must retain the funds until consent has been given by FIC to return the funds to the source they came from.

4.4 Simplified client due diligence – Low-risk clients

Simplified procedures apply for low-risk clients as depicted in TABLE 1 above. The following types of clients are considered lower risk:

- a. Credit or financial institutions regulated by the European Directive 2005/60/EC and its relative transposition member countries legislation on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.
- b. Credit or financial institutions situated in a third country which imposes requirements equivalent to those laid down by the European Union (the EU equivalent jurisdictions) and are under supervision for compliance with those requirements.
- c. Listed companies whose securities are admitted to trading on a regulated market of an EU member state or EU equivalent jurisdictions which are subject to disclosure requirements consistent with accepted legislation.
- d. Domestic public authorities of countries of the European Economic Area.

The Company may apply a simplified due diligence procedure, and not the following client identification and due diligence measures, in respect of the Low-Risk Clients:

- a. identifying the client and verifying the client's identity based on documents, data or information obtained from a reliable and independent source.
- b. identifying the beneficial owner and taking risk-based and adequate measures to verify the identity based on documents, data or information obtained from a reliable and independent source so that the person carrying on in financial or other business knows who the beneficial owner is; about legal persons, and similar legal arrangements, taking risk based and adequate measures to understand the ownership and control structure of the client.
- c. obtaining information on the purpose and intended nature of the business relationship.
- d. conducting on-going monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the information and data in the possession of the person engaged in financial or other business in relation to the client, the business and risk profile, including where necessary, the source of funds and ensuring that the documents, data, or information held are kept up to date.
- e. the verification of the identity of the client and the beneficial owner is performed before the establishment of a business relationship or the carrying out of the transaction.

With reference to the above it is also clarified that EU equivalent jurisdictions are those third countries outside EU jurisdictions which impose procedures and take measures for preventing money laundering and terrorist financing equivalent to those laid down by the European Directive 2005/60/EC and as such are of low AML risk (see Appendix 3).

It should be noted that the Company gathers sufficient information to establish if the client qualifies to be classified as lower risk client.

The Company does not apply simplified due diligence where, despite the client falling in one of the above categories, there is a risk of money laundering activity.

It is clarified that the term subsidiary applies where the parent company can exercise considerable influence and control over its operating and financial policies; this would usually be the case where the parent controls over 50% of the subsidiary's voting rights and/ or has the right to appoint the majority of the Board.

Where the Company applies simplified due diligence measures it requires the collection of the following documents:

- a) Proof of regulated status e.g., copy of the licence.
- b) Certificate of incorporation.
- c) Board resolution for the opening of the account.
- d) POI and POR from the authorised person/s to operate the account.
- e) Latest Audited Financial Statements (where applicable).
- b) The entities need to complete the Company's "Account opening form" and World check is performed for all natural persons involved.

4.5 Enhanced client due diligence – High-risk clients

As mentioned above, since the vast majority of the Company's clients are non-face-to-face, they are by default categorized as High-Risk. For ascertaining the true identity of such customers, the Company obtains the following information:

- a) True name as stated on the official identity card or passport.
- b) Full residential address, including postal code.
- c) Telephone and Email address.
- d) Date of birth.
- e) Nationality.
- f) Details of profession and other occupations of the customer.

The Company takes additional measures when conducting client due diligence in cases where there is elevated higher risk of money laundering and the client is considered as High-Risk by:

- Performing searches on the database of World Check to identify sanctioned individuals or entities as well as verifying passport authenticity. All potential clients need to be screened against international databases through World Check to identify potential matches.

- Assessing whether the type of the natural or legal person falls under one of the high-risk categories as described above under Table 1.

Specifically, the Company requests for the following documents during the on-boarding procedure to verify the above information of the client:

- a) A valid proof of identity; the Company requests for international passports; where the potential client is unable to provide it with a passport the company may collect a national ID or driver's license. The potential client is advised to provide the Company with an international passport as soon as practicable.
- b) Recent proof of residence, in the form of a utility bill, local tax authority bill or a bank statement (not older than 3 months).
- c) Completes satisfactorily the financial information section in the account registration based on which the client's economic profile is constructed.
- d) Checks such clients against Worldcheck or equivalent online AML databases and internet search engines (including standard Google searches, LinkedIn, or equivalent databases) to identify validity of passport and validity of economic profile provided on the account opening portal, PEP status, involvement in any illegal activities, inclusion in any sanctions lists, etc.) Performing a World Check is very important for the compliance procedure. The compliance status of an account **cannot** be changed without performing a World Check on a customer's profile.
- e) Requires that deposits to the client's account are always from a source in the name of the client which is not subject to any international sanctions and withdrawals are always to the source from which the deposit was received. In case where this is not possible (e.g., credit card refund is not possible because a year since deposit has passed) withdrawals may be executed to a source in the name of the client.

Furthermore, the Company conducts monitoring of the business relationship through reviews of the client's trading activity, deposits/withdrawals, and online searches as these are described in Section 8.2 of the manual. (Customer Due Diligence – CDD)

4.6 Standard Client Due Diligence- Medium Risk Clients

The Company considers as Medium Risk those clients who do not fall under the Low or High-Risk categories. The client types falling under the Medium Risk category are shown in TABLE 1 above.

The due diligence procedures the Company applies on all medium risk clients in order to compensate for the elevated risk versus the low-risk clients include the following:

- a) Ensuring that the client's identity is established by additional documents, data, or information.
- b) Verifying the documents supplied or requiring confirmatory certification by 3rd party independent sources.
- c) Check all Medium Risk clients against "World-check" database and internet search engines to identify validity of identity documents, passport, PEP status, involvement in any illegal activities, inclusion in any sanctions lists, etc.

- d) Conducting enhanced and continuous monitoring of the business relationship.

4.7 Approval of clients

The approval of clients is performed by the Company's verification department under the supervision of the Head of Back office and monitored by the MLRO and relevant records/statements are properly recorded online in the Company's system. Corporate accounts and joint accounts can only be established and confirmed as compliant following the approval of the MLRO.

5. CLIENT'S ECONOMIC PROFILE

The client's economic profile is constructed, initially, through completion of the account opening portal data fields. Subsequently, and subject to its risk-based approach, the Company may request additional information should it consider that clarifications are required for a better understanding of the client's profile. The Company may also require the updating of the economic profile as part of its reviews on high-risk clients. The Company requires the construction of the economic profile of all its clients irrespective of risk categorization exceeding the requirements of the Law.

The economic profile questions included in the 'Account Opening Procedure' include the following:

- a) purpose and reason for requesting the establishment of a business relationship.
- b) the anticipated account turnover.
- c) nature of transactions.
- d) expected origin of incoming funds to be credited in the account.
- e) the customer's size of wealth.
- f) annual income.
- g) employment status.
- h) industry/Source of funds; and the
- i) origin of funds.

It is noted that for legal persons, the data and information that are used for the construction of clients' economic profile include, inter alia, the name of the company, the country of its incorporation, the head offices address, the names and the identification information of the beneficial owners, directors and authorized signatories, financial information, ownership structure of the group that the company may be a part of (country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information).

The said data and information are recorded electronically in a separate section designed for this purpose which is retained in the customer's file in the Company's clients' database along with all other documents. The said form is updated whenever new information emerges that needs to be added to the economic profile of the customer or alters existing information that makes up the economic profile of the customer.

The Company has the right not to proceed with the establishment of a business relationship or execution of an occasional transaction or can terminate a business relationship with a prospective client in case the client fails or refuses to submit the requested information for the verification of his identity and the creation of his economic profile.

The information contained in the Account Opening Procedure as regards the economic profile of the client is reviewed by the MLRO as part of the client ongoing review process and is used as reference when comparing client account activity with the client's representations.

6. CLIENT IDENTIFICATION – Additional Guidance

The purpose of these procedures is to ensure that the Company is in a position to be able to say, "We know our client". The procedures are set out in table form in Appendix 7 the "Client Identification Checklist" and below, and they are aimed to ensure that our clients actually exist and that they are who they say they are. The overriding requirement is that the Company is satisfied that it has established the true identity of the prospective client/investor as far as it is reasonably possible.

The Guidance Notes as referenced in Appendix 14 are the principal source for developing appropriate procedures. However, they provide some room for the exercise of discretion in carrying out their recommendations. Such discretion must be exercised only by the MLRO and with great caution, as its exercise may well be the subject to subsequent review by persons armed with much more information than we had at the time of entering into the business relationship with the client.

What is identity: An individual's identity comprises his/her name and all other names used and address at which he/she can be located. Date of birth is also a useful indicator of identity. To identify somebody, an official document bearing a photograph of the person (e.g., certified copy of a passport or driving licence) should be obtained.

Corporate identification should include obtaining of incorporation documents, independent verification of the existence of the corporate body and confirmation that it exists for a legitimate purpose. Any subsequent changes to a customer's identification that are brought to the attention of the Company should be recorded as part of the KYC process.

Methods of Identification:

In terms of FICA, an accountable institution may **not** establish **a business relationship** or conclude **a single transaction** with a client or prospective client unless it has taken certain prescribed steps to establish and verify the identity of the client or prospective client, as the case may be. Identification of the "principal" and "agent" and proof of authority are required where the client is acting on behalf of someone, or someone is acting on behalf of the client.

“**A business relationship**” in FICA is defined as “*an arrangement between a client and an accountable institution for the purposes of concluding transactions on a regular basis*”.

“**Transaction**” is widely defined in FICA as “*a transaction concluded between a client and an accountable institution in accordance with the type of business carried on by that institution*” and is not limited to transactions involving the flow of money.

6.1 Identification of Individuals

The following information should be obtained and verified:

Identity notarised or certified copy of signed identification papers with a photograph attached such as a passport, drivers’ licence, or national identity card. We must ensure that these papers remain valid and have not expired and that there is no variation in the signatures used on the identification papers and the subscription document for the fund.

Address. We must obtain two of the following:

- a. original or certified copy of a utility bill.
- b. original or certified copy of a mobile telephone bill.
- c. original or certified copy of an insurance bill; or
- d. original or certified copy of a bank, building society or financial institution statement.

In our procedure, we seek to ascertain who the investor is, and therefore the following information is vital:

- a. full names used.
- b. date of birth.
- c. place of birth.
- d. nationality.
- e. occupation.
- f. specimen signature; or
- g. current permanent residential address, including zip or postal code.

6.2 Identification of Ultimate Beneficial Owners (UBOs)

Entities

The use of corporate entities and trusts raises specific issues in AML laundering procedures because the identity of the UBO is obscured by the corporate or legal structure of the entity. The principal aim of our identification procedures here is to penetrate the corporate entities and identify those persons who have ultimate

FRONTIER MARKETS (PTY) LTD, Registration number 023/780267/07 is a private company incorporated in accordance with the laws of South Africa an authorised Financial Services Provider registered as such in terms of the Financial Advisory and Intermediary Services Act, 2002 under FSP No. 53333

FRONTIER MARKETS Pty Ltd Address 11 WALNUT ROAD, DURBAN CENTRAL, DURBAN, KWA-ZULU NATAL, 4001

control over the assets. Particular attention should be paid to anyone who has contributed significant capital to the investing entity. Additionally, every effort must be made to ensure that the investing entity exists for a legitimate trading or economic purpose.

Companies

We will inspect the incorporation documents such as the following documents to satisfy ourselves of the investor is *bona fides*:

- a. certified copy of the certificate of incorporation.
- b. certified copy of a Certificate of Good Standing from Registrar of Companies.
- c. certified copy of the memorandum of Incorporation (or equivalent).
- d. an authorised signatory list of the fund.
- e. a list of directors' names, occupations, residential and business addresses, and dates of birth **and** in the case of a Fund from a country listed in Appendix 6, identification papers as outlined in 6.1 above of at least 2 directors of the Fund; and
- f. in the case of a fund from a country **not** listed in Annexure A identification papers as outlined in 1 above of all the directors of the fund **and** names and addresses of beneficial owners of the fund holding 10% or more of the issued share capital of the Fund.

Anyone who is to be authorised to sign on behalf of a Fund must be duly authorised by the Fund. You should seek evidence of this authorisation.

Partnerships (including a Business Partnership and a Limited Partnership)

The following documents should be obtained:

- a. a certified copy of the mandate governing the partnership or the partnership agreement; and
- b. in the case of a Business Partnership identification papers as outlined above for each partner; or
- c. in the case of a Limited Partnership from a country listed in Annexure A, identification papers as outlined above of the General Partner; or
- d. in the case of a Limited Partnership **not** from a country listed in Annexure A, identification papers as outlined above of the General Partner **and** all underlying partners; and
- e. an authorised signatory list of the Business Partnership or General Partner.

Trusts

In the case of trust accounts the following should be provided to establish the identity of the trustee and the beneficiaries of the trust:

- a. a list of trustees; and
- b. their occupations, addresses and date of birth; and
- c. a copy of the Trust Deed; and
- d. an authorised signatory list; and
- e. a list of beneficiaries of the trust and certified ID documents for the beneficiaries; and

FRONTIER MARKETS (PTY) LTD, Registration number 023/780267/07 is a private company incorporated in accordance with the laws of South Africa an authorised Financial Services Provider registered as such in terms of the Financial Advisory and Intermediary Services Act, 2002 under FSP No. 53333

FRONTIER MARKETS Pty Ltd Address 11 WALNUT ROAD, DURBAN CENTRAL, DURBAN, KWA-ZULU NATAL, 4001

- f. identification papers as outlined above of the donor of the Trust.

Limited Liability Corporation (LLC)

In the case of an LLC the following documents should be obtained: -

- a. a certified copy of the LLC agreement; and
- b. in the case of an LLC from a country listed in Appendix 3, identification papers as outlined above of the managing member; or
- c. in the case of an LLC **not** from a country listed in Appendix 3, identification papers as outlined in 6.1 and 6.2 above of the managing member **and** all other members; and
- d. an authorised signatory list of the managing member.

6.3 Politically Exposed Persons (PEP)

A PEP is a term used for an individual who is a politically exposed person or has in the past performed prominent public functions in any particular country. The principles issued by the Wolfsberg Group of Leading International Financial Institutions give practical guidelines on these issues. These principles are applicable to both domestic and international PEP's. Establishing business relationship with persons who have important public positions or political offices or their 'associates' as defined in FAIS, entails additional risks that the Company should assess.

Checks must be performed in relation to the potential client in World Search databases in order to identify if the respective potential client is considered a PEP or is included in any sanctions list.

The meaning of PEP includes, but is not limited to, the following natural persons who are or have been entrusted with prominent public functions:

- 1. Heads of state, heads of government, ministers and deputy or assistant ministers.

2. Members of parliaments, Members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except exceptional circumstances.
3. Members of courts of auditors or of the boards of central banks, Ambassadors, chargis d'affaires, and high-ranking officers in the armed forces.
4. military leaders.
5. members of royal families.
6. senior and/or influential representatives of religious organisations; and
7. members of the administrative, management or supervisory bodies of State-owned enterprises. Note: None of the above shall be understood as covering middle ranking or more junior officials.

The Company will conduct proper due diligence on the PEP's and any person acting on their behalf, and PEP's personally or acting on behalf of family members will be subject to scrutiny. In terms of FICA, specific action should be taken in respect of PEPs as a category of high risk clients. The PEP is immediately a high risk client.

In addition to performing the usual risk management measures, the Company will put in place a proper risk management system to determine whether the client is a PEP. In addition, the Company employees must obtain approval from the MLRO before approving the establishment of a business relationship with a PEP and will take reasonable measures to establish the source of wealth and the source of funds and will conduct enhanced on-going monitoring of the relationship with the PEP.

6.4 New Clients

Accordingly, the Company's policy towards identification of PEPs and its due diligence process prior to the establishment of a business relationship is as follows:

1. The Company will perform checks regarding the potential client's name against a database available in the market in order to identify whether the potential client is considered a PEP or is included in any sanctions list.
2. When a potential customer is identified as a PEP, he is categorized as a High-Risk client and the Company cannot proceed with the establishment of the business relationship prior to conducting full due diligence as per the below:
 - a. The Company obtains adequate documentation to establish the identity of the PEP and to assess his/her business reputation. To this extent, the Company collects:
 - i. Proof of identity, same as the documents collected for natural persons.
 - ii. Proof of residence, same as the documents collected for natural persons

- iii. Application of at least one enhanced due diligence measure.
 - iv. Reference letter from a reputable third party (such as an international Law or Accounting Firm) to assess the business reputation of the PEP.
 - v. Source of funds and construction of economic profile. The Company recognises the heightened importance of having in place a rigid and comprehensive understanding of the source of wealth of the PEP and of the funds intended to be traded through the Company. In this respect, and whilst for all clients' information is gathered on the economic profile of clients and their sources of wealth, in the case of PEPs the Company undertakes enhanced measures including indicatively ensuring proper tax declarations of the PEP in his country of residence, matching of the economic profile of the PEP to his income from the PEP position held and business activities, and seeking detailed clarifications from PEPs about their sources of wealth etc. It is of foremost importance that this economic assessment is completed to the satisfaction of the MLRO.
 - vi. Online reputational research is performed on the potential customer to identify any adverse media, including whether the PEP has been the subject of any tax investigation, any bribery or corruption scandal or similar situations.
- b. Upon collection of all the information and documentation, the Head of Verification Department at the Company forwards the request for the establishment of an account along with the collected information and documentation to the MLRO for review.
 - c. The MLRO will request further information as appropriate, including either the conducting of an in-person meeting with the PEP or holding a relevant skype or conference call, unless the PEP is personally known to a member of the management team of the group who are asked to provide in writing their knowledge and view of the PEP and on the establishment of a relevant business relationship.
 - d. The approval by both the Executive Director (preferably the CEO) and the MLRO are required for the establishment of a business relationship or the execution of any transaction with a PEP. Such approval is decided on the basis of a profile on the PEP which includes as a minimum the following:
 - a) jurisdiction.
 - b) business profile.
 - c) source of funds and wealth.
 - d) information available from public sources.
 - e) payment methods used for depositing and withdrawals. The Company only accepts methods on the name of the client.
 - f) "World-check" on the PEP and any other information in the Company's possession.
 - e. The decision of the Executive Director and the MLRO along with the basis for the decision shall be documented in writing (Appendix 4).
 - f. In a substantial number of cases, PEPs operate through complex legal structures such as offshore special purpose vehicle, most frequently also administrated by nominee shareholders and directors. In all cases, the work to be done should cover two axes:
 - Identification and verification of the PEP, by carrying out all the work outlined above.
 - Identification and verification of the entity that applies to become the Company's client, including the nominee shareholders and directors, in accordance with the due diligence procedures outlined within this policy for the specific types of entities. Where any of the nominee shareholders (over 10%) or directors / trustees are not of a good repute (e.g., perfect match on World Check, do not have any professional registration, negative market feedback etc.) the Company will reject the establishment of the relationship with the PEP.
 - g. In all cases outlined above, the bank accounts from which the PEP or the legal structure remits funds to the Company should be established in the name of the client (natural or legal person as appropriate) at a regulated bank in an approved jurisdiction of low AML risks.

Existing clients

When the business relationship has already been established with a customer (natural or legal person) and subsequently it is ascertained that the persons involved are or have become PEPs, then an approval is given for continuing the operation of the business relationship by the Executive Director of the Company and the MLRO. During the review period, the Company shall request and collect the required documents as these are collected during the approval process of a PEP as a new customer. An existing client who fails to comply with the Company's request within 1 month from the request shall be immediately terminated.

All PEPs' due diligence information and documentation are subject to an annual refresh / update review.

Ongoing monitoring

Each PEP account and its movements are monitored closely as part of the Monthly AML Monitoring and are reported in the monthly report. The monitoring includes measures to understand the source of wealth of the client and source of funds for the transactions and such information is documented in the client's file and crucially whether the transactions undertaken in the month correspond to the Company's understanding of the PEP's intended transactions when opening the account with the Company. The MLRO also on an annual basis prepares a report referring to the PEP client account activity and any update about the PEP and submits it to the Board of Directors with his/her recommendations as to whether the Company should continue its business relationship with each PEP client. The Board's approval is required if the business relationship with the PEPs is to continue.

6.5 Joint accounts

In case of joint accounts, the identity of all individuals that hold or have the right to manage the account are verified in accordance with the requirements for natural persons prescribed in this policy. Joint accounts are considered of higher risk by the Company and further information and documentation may be requested where the Company deems it appropriate.

The Company establishes joint accounts solely for spouses and civil partnerships and for first degree relationships (parent-child, siblings). The Company does not establish joint accounts of 3 or more people. The clients must choose the main account from which they will trade.

All requested information must be provided to the Company prior to the creation of the joint account. Joint Account Application Form in Appendix 5 must be duly signed by the clients and match the details provided in Personal Details documentation. In the Joint Account Application Form the clients must agree to be jointly and severally responsible for the Account and must acknowledge that they have read and understood the Company's terms and conditions.

6.6 Anonymous or Numbered accounts

FRONTIER MARKETS (PTY) LTD, Registration number 023/780267/07 is a private company incorporated in accordance with the laws of South Africa an authorised Financial Services Provider registered as such in terms of the Financial Advisory and Intermediary Services Act, 2002 under FSP No. 53333
FRONTIER MARKETS Pty Ltd Address 11 WALNUT ROAD, DURBAN CENTRAL, DURBAN, KWA-ZULU NATAL, 4001

The Company does not establish anonymous or numbered accounts. Additionally, the Company pays special attention to any money laundering or terrorist financing threat that may arise from products or transactions that might favor anonymity and takes measures to prevent their use for money laundering or terrorist financing purposes.

6.7 non-acceptable clients

The Company does not approve the establishment of a business relationship with natural or legal persons engaged in illegal activities such as arms dealing and drug trafficking.

In order for the Company to assess whether to accept or reject a client, it also takes into consideration factors such as the client's background, type and nature of its business activities, its country of origin, the anticipated level and nature of trading activity as well as the source and origin of funds.

In addition, the clients who are residents of a restricted jurisdiction are not accepted by the Company. All the high-risk countries in accordance with the FATF recommendations are indicated as restricted jurisdictions in the Company's websites' terms and conditions from which the Company does not accept clients. The list may be amended from time to time depending on the updates from the FATF.

6.8 Lead and Practice Account

Lead is a registration created in the Company's CRMBO when the customer is only registered at the website without completing the full account registration procedure. The potential client at this stage cannot deposit nor trade and is not yet considered a Company's client.

Practice account is a demonstration (demo) account which the customer registers for and provides a risk-free account that simulates real trading conditions which is active for the period of 30days.

Since both, lead, and practice accounts, are not real accounts the Company does not obtain and complete the KYC verification process.

6.9 Deceased client

In cases of deceased clients, the following procedures shall be followed:

A. In case of active bank account on the name of the deceased:

The heirs should provide letters of executorship, their death certificate, their certificate of inheritance and their POI. Afterwards a withdrawal request form should be submitted. The Company shall transfer the money to the deceased bank account.

B. In case of no active bank account:

– In this case the funds can be paid to a bank account owned by an heir.

The Company shall receive:

– Letters of Executorship.

– Death Certificate.

– Certificate of Inheritance.

– POI of all heirs.

– Notarized document, showing that all the heirs agreed the money from the Company to be paid to a specific bank account owned by one of the heirs or to the Notary.

If one of the heirs is underage, a certificate showing who is the guardian and the POI of the guardian together with the POI of the underage heir will be collected.

6.10 Underage clients

The Company in complying with the Law as amended does not accept minors, i.e., persons below the age of 18, as clients. Where an underage person signs up electronically for the creation of an account by providing the Company with false and/or fake details, the Company, as soon as it becomes aware of this, must terminate and/or close the account of the underage person immediately.

An underage person is not entitled to enter into any contracts and/or engagements under the law, and they are perceived as not having a business relationship with the Company. Upon the Company receiving knowledge that a person is underage, the Company will inform them through email and/or telephonically, that the Company is unable to accept them as clients since they do not match the Company's profile and that any money deposited in their trading account will be refunded to them in the same way a deposit was made.

Should it be impossible for the Company to refund the underage person in the same way the deposit was made, then the underage person needs to provide the Company, following a request, with a bank account to which they are the beneficial owners. In case, the underage person does not have a bank account to which they are a beneficial owner, the underage person's parent and/or legal guardian must be contacted.

The parent and/or legal guardian must provide the Company with the following:

FRONTIER MARKETS (PTY) LTD, Registration number 023/780267/07 is a private company incorporated in accordance with the laws of South Africa an authorised Financial Services Provider registered as such in terms of the Financial Advisory and Intermediary Services Act, 2002 under FSP No. 53333
FRONTIER MARKETS Pty Ltd Address 11 WALNUT ROAD, DURBAN CENTRAL, DURBAN, KWA-ZULU NATAL, 4001

- a. POI such as a valid passport or ID; and
- b. Official documentation proving the relationship between the underage person and the parent and/or legal guardian such as a birth certificate; and
- c. Bank account to which the parent and/or legal guardian is a beneficial owner.

As soon as the Company receives the documents from the underage person's parent and/or legal guardian and the underage person confirms return of the money to the parent's and/or legal guardian's bank account, the Company must refund the money deposited by the underage person to the parent's and/or legal guardian's bank account.

Should the customer wish to open an account upon turning 18 years old, a new account must be created.

6.11 Reliance on third parties for KYC identification

Recognizing that the client has the ultimate responsibility for client identification, it is the Company's policy not to rely on third parties for KYC identification, where third party means credit/financial institutions, auditors, legal professionals, trust, and corporate services providers.

7. DOCUMENTATION

7.1 Documentation standards

The Company, given the nature of its business, collects copies of the documents.

However, where the MLRO deems it appropriate due to the increased risk, identification documentation needs to be in their original or in certified true copy form. Certified true copy means that the person certifying the copy of the document has seen the original document and is in a position to certify that the copy is a true and complete copy of the original document.

Client identification documentation obtained at the account opening stage or during client file reviews should be recent (where applicable) and always up to date. Documents relating to the verification of the client's permanent address and bank references are considered as recent when submitted to the Company within 3 months from the issue date. Detailed information regarding the specific documentation collected depending on the type of the potential client is indicated in **Appendix 7.**

7.2 Supporting documentation:

FRONTIER MARKETS (PTY) LTD, Registration number 023/780267/07 is a private company incorporated in accordance with the laws of South Africa an authorised Financial Services Provider registered as such in terms of the Financial Advisory and Intermediary Services Act, 2002 under FSP No. 53333
FRONTIER MARKETS Pty Ltd Address 11 WALNUT ROAD, DURBAN CENTRAL, DURBAN, KWA-ZULU NATAL, 4001

A. Proof of ID can be demonstrated through any of the following documents: **Passport, national identification card (ID card), or driver's license.** **Valid POI** must fulfil the following criteria:

- **Full Name** – same as in the CRM (Back Office). In case it differs, it needs to be verified over the phone.
- **Date of Birth** – same as in the CRM. In case it differs, it needs to be verified over the phone.
- **Expiry Date** – must be valid. If the POI expires in less than a month, it cannot be accepted, and client should be requested to send another POI.
- **Picture** should be **clear**.
- **All the details** on the POI must be clearly **visible**.
- **Both sides** of the ID documents are needed – **front** and **back** (where applicable).

The Company as a default, requests potential clients to provide it with a copy of their international passport. Where this is not available, potential clients may provide the Company with a copy of their ID card or driver's license but must provide the Company with a copy of their passport once available.

B. Proof of address can be demonstrated through any of the following documents: Utility Bill (internet, television, water, electricity, landline phone), bank or credit card statement, local tax authority bill or an equivalent document.

Valid POR must fulfil the following criteria:

- **Full Name** – same as in the identification document.
- **Address** – same as the residence address in the CRM. In case the address is different, we need address verification over the phone.
- **Issued date** – **not older than 3 months**. Any POR older than 3 months will not be accepted.
- **Official POR** with **Logo** and/or **stamp**.

The following documents **cannot be accepted** as POR:

- SWIFT.
- Wire Transfer Document in handwriting.
- Courier Bill.
- Other document in handwriting unless it is a government issued doc with stamp and signature.
- Envelopes.
- Editable WORD documents.

Where the client is unable to provide a POR in the prescribed methods indicated above, the Company may accept a document produced, signed, and stamped by the municipality verifying the clients' or potential clients' residency.

7.3 Document verification

Depending on the type of document, the Company takes the necessary steps to confirm the authenticity of documents and information provided by potential clients as follows:

- i. For verification of the authenticity of the document of the potential client's Proof of Identity the following are used:
 - a) check how the actual document looks, by checking evidence of watermarks and security elements via the following websites or google:
 1. <http://www.documentchecker.com/> (Keesing).
 2. <http://www.consilium.europa.eu/prado/en/search-by-document-country.html>.
 - b) run a World Check on the Machine-Readable Zone (MRZ) line of an identity card or passport in order to determine authenticity (where applicable).
 - c) confirm validity of the MRZ (Machine Readable Zone) line via Keesing.
 - d) where applicable and/or possible, check in governmental websites in terms of the document's authenticity; and
 - e) where possible, proceed with Google/Facebook search on the name/email of the potential client, to identify real pictures matching the one on the proof of identity.
- ii. For verification of the authenticity of POR the following are used:
 - a) perform a Google search on the issuing company of the proof of residence.
 - b) run a google street view where possible; and
 - c) run a Facebook search.

7.4 Reliable/ independent authenticators for document certifications

Reliable authenticators are authenticators from which the Company will accept document certifications as true copies:

- a Regulated Financial Institution from an EU or EU equivalent jurisdiction provided the authenticator is of a relevant position (director, management, compliance, legal, secretariat, operations).
- a licensed lawyer, auditor, fiduciary services provider, fund administrator, notary public, from an EU or EU equivalent jurisdiction.
- the Embassy or Consulate of the client's home country in the Republic of South Africa.
- the Embassy of the Republic of South Africa in the client's home country.
- the Police.
- a Company Registrar in an EU or EU equivalent jurisdiction.

- any full-time employee of the Company; and
- the national courts.

7.5 Language of documentation

The Company may receive documents from customers in any language. Where the documents are in a language other than English, a true translation is required. Translations may be performed by employees of the Company or its group who are proficient in both English and the translated language. In cases where there are no employees who are proficient in the translated language, a true translation in English language should be provided. The name and capacity/position of the person translating the document as well as the date of the translation, initial language of the document and the signature needs to be indicated on the document through the required stamp. Translations are attached to the original text.

Through the translation, the Company needs to be in a position to obtain the following information:

- i. Proof of Identity – all information needs to be translated and particularly (as applicable) the:
 - a. Name
 - b. Date of issuance
 - c. Date of birth
 - d. Place of birth
 - e. Name of issuing authority
 - f. Date of expiry (where applicable)
 - g. Type of document
- Proof of residence – all information needs to be translated and particularly (as applicable) the:
 - a. Name
 - b. Date of issuance
 - c. Address
 - d. Type of document

8. ELECTRONIC VERIFICATION

The Company may verify its clients' information electronically, through legitimate third-party data providers. It is to be noted that any third parties engaged for electronic verification purposes are subject to prior enhanced due diligence to ensure that they are fit and proper to offer such services to the Company and have the right credentials, expertise, and track record in such electronic verification services. The assessment is done by the MLRO with the approval of the Compliance Officer.

In order for a client to be verified electronically, information must come from two or more electronic sources. The procedure satisfies the following correlation standard:

- (a) Identification of the customer's full name and current address from our source, and
- (b) Identification of the customer's full name and either his current address or date of birth from a second source

In addition, the customer must successfully pass the online screening against sanctions and PEPs lists.

If a client fails electronic verification, the Company may enable the client to be verified through the production of documents.

9. AML/KYC MONITORING PROCEDURES

9.1 Updating clients' files

The Company is required to carry out on-going monitoring of the business relationships established with clients. On-going monitoring is performed by the Company in order to ensure that the account activity is in line with the information that the Company obtained for the construction of client's economic profile and in order to identify any suspicious transactions. As part of monitoring procedures, the Company is further under an obligation to request to update the documents kept for due diligence purposes.

The Company ensures that the information and documentation obtained for the client identification and for the construction of his economic profile remains updated throughout the business relationship.

Where the Company becomes aware that valuable information pertaining to a client has changed, it requests the relevant details from the client. Valuable information includes but is not limited to:

- a. a significant transaction takes place which appears to be unusual and/or significant compared to the normal pattern of the transactions and the economic profile of the client.
- b. a material change in the way and the rules under which the client's account operates such as a change of the persons that are authorized to operate the account.
- c. in the case of a corporate client, a material changes in the clients' legal status and situation such as:
 - change of directors/secretary.
 - change of registered shareholders and/or beneficial owners.

- change of registered office.
- change of trustees.
- change of trading and/or corporate name; and
- change of the principal trading partners and/or undertaking new major business activities.

The Company's policy is to review all High-High risk clients' files on an annual basis. For High-Medium risk clients the files are reviewed on a two-year basis and for the High- Low Risk clients the review is performed every three years. The results of the review are documented on each file and saved electronically using the form. In the event where any of the KYC documentation is no longer valid, the Head of Back Office, following instructions from the MLRO, shall request the client to provide it with updated documentation.

It is clarified that in order to make best use of the Company's resources, only active clients (non-dormant) are reviewed (i.e., clients who had trading activity in the last 90 days). In the case of no activity the client is disabled from further trading and may only resume trading on submission of updated client identification information.

The MLRO may consider reporting noncomplying clients to FIC in case there are reasonable grounds to believe that such clients relate to money laundering and terrorist financing activities.

9.2 Ongoing monitoring of clients' trading activity

The Company is required to carry out on-going monitoring of the business relationships established with clients. On- going monitoring is performed by the Company in order to ensure that the account activity is in line with the clients' economic profile and in order to identify any suspicious transactions.

The procedures and frequency of monitoring of clients' trading activity is risk based. In this respect, the Company monitors high risk material clients with particular emphasis to those with high trading volumes, high deposit, and withdrawals volumes. The monitoring exercise involves comparing the client account turnover against anticipated figures based on the clients' economic profile as set out at the onboarding stage. Material variances, from expected levels of trading, together with particularly complex, suspicious, or highly unusual transactions and deposits/ withdrawals without any apparent economic reason are investigated by the Company. A more detailed list with examples of suspicious transactions can be found below (Appendix 12).

The procedure followed for the monitoring of clients' transactions are analyzed below:

1. Monthly review of the Top 15 depositors per month.
2. Sample check of 50 clients per month.

3. Use of a risk management tool for the monitoring of credit card deposits and identification of suspicious activity. The system is configured in coordination with the Company's processor and includes triggers (54) and filters (40) providing alerts. Triggers provide alerts which are subject to review by the Company whilst having no effect on the transaction itself. Filters block a deposit from reaching account thereby permitting the Company to ensure blocking of certain activity.
4. **SAS AML system for ongoing monitoring on transactions.** The system provides alerts upon triggering of a specific scenario. The alerts can be closed, suppressed, investigated as suspicious and reported as suspicious. Scenarios include:
 - a. Scenario 1: High deposits and no activity for 30 days. The scenario generates an alert when a customer makes a high deposit (minimum of R25,000.00) and has no activity for the following 30 days.
 - b. Scenario 2: Unusual trading activity during the 30 days: the scenario is examining unusual trading behavior in a period of 30 days compared to the average of the same customer's activity during the last 6 months.
 - c. Scenario 3: Unusual cash flow behavior: the cash flow is compared to the data stated during the account opening procedure. The scenario gives an alert with a lookback period of 30 days. The total aggregated cash flow is a minimum of R [●] [Daniel to confirm this amount and the currency depending on internal processes] and this represents minimum 25% of the customer's annual income as indicated during account registration.
 - d. Scenario 4: Unusual trading behavior compared to Per group activity: this scenario compares trading activity of customers with the same characteristics.

The system includes 3 additional risk factors, which raise the risk scoring of an alert once such is generated from each of the scenarios. The system is still under construction.

5. In addition, all deposits, and withdrawals equal or exceeding R25,000.00 must be reported to the MLRO for review prior to the crediting of the deposit or execution of the withdrawal request.

9.3 Funds transfers (Deposits & Withdrawals)

Recognizing the AML risks associated with 3rd party funds transfers and considering the risks associated with its clients being non-face to face the Company decided to prohibit any 3rd party deposits and 3rd party withdrawals.

Specifically, the Company requires that deposits to the client's account are always from a payment method in the name of the client and withdrawals are always to the same source from where the deposit was received.

Deposits from joint bank accounts:

When the Company receives a deposit from a Joint Bank Account, the following documents shall be collected by the Company:

- a. POI of both parties:

- i. carry out a world check for both parties; and
 - ii. POI of the third party must contain a signature.
- b. Joint Bank Account Declaration Form completed by the third party (**Appendix 8**)

Upon receipt of the Joint Bank Account Declaration Form the Company must ensure that the form is signed by the third party by comparing the signature of the form with the signature on the third party's POI.

Withdrawals:

Withdrawals are permitted following the submission of a withdrawal request by the customer through the relevant procedure indicated on the Company's websites under the "HELP" feature. Withdrawals as a default are performed to the same source as the deposit was made. Should the initial bank account or other payment method (e.g., client's credit card has expired) be no longer available for withdrawal the Company will proceed with a withdrawal to a bank account in the name of the client, which the client shall indicate. The client will need to provide proof of the unavailability of the initial deposit method. Withdrawals to third parties are as a default not permitted and may only be performed in exceptional cases, following senior management approval.

Cash Transactions

In a further effort to eliminate AML risks the Company **does not accept** cash deposits or withdrawals in any form.

In particular, the Company has liaised with the credit institutions it collaborates with in order to block the acceptance of cash deposits. Certain banks such as ALPHA BANK S.A, Emirates NBD, ALPHA BANK (Romania) etc. continue to accept cash deposits from the Company's clients irrespective of the instruction provided by the Company since they are unable to block cash deposits due to technical constraints.

In cases where the Company receives a cash deposit either in a single operation or in several operations in any of its bank accounts due to inability of the bank to block cash deposits or for any other reason it must proceed as follows:

- i. The Company requests the collection of all supportive documentation from the client to verify the source of funds including the **declaration of cash deposits form DOCD** (please refer to **Appendix 9**), **swift confirmation** indicating the deposit of the funds by the client, **supportive evidence as indicated on the declaration of Cash deposits form**, to support the information regarding the source of funds indicated by the client and all the **KYC documents** in the event which the client has not yet provided them.

- ii. Upon receipt of the documentation all cash deposits regardless of the amount, are reported to the MLRO for review.
- iii. The Company may refund clients with the amount of cash deposits accepted to a bank account on the depositors' name, unless following review by the MLRO, a report to FIC must be made. In such a case, the Company may not proceed with refund until a decision has been notified to the Company by FIC in relation to the handling of the funds. The reporting to FIC will be performed following receipt of all the aforesaid documentation. Once FIC provides the Company with a decision the Company needs to act accordingly.
- iv. The Company must not show the funds as available ("balance") in the client's account (hence no transaction can take place).
- v. As a policy the Company reports to FIC all cash deposits received equal or exceeding the amount of R25,000.00
- vi. The MLRO prepares an investigation form (Appendix 10) indicating the findings including a decision to report to FIC and/or return the funds which is kept electronically and in hard copy in the Company's records.

Cash deposits equal or exceeding R25,000.00 are included in the Company's Monthly prevention statements to FIC.

Funds received in one of the Company's bank accounts from an Exchange Company are considered of equivalent risk as cash deposits. To that extent, the Company does not accept such deposits and handles them in the same way as cash deposits specified above.

Restrictions on incoming and outgoing payments

The Company does not accept any incoming funds and does not perform any outgoing payments to any countries subject to sanctions in terms of *Guidance on the Offence of Financing of Terrorism and the Financial Sanctions Regime for Bodies Designated under Section 32 of the Criminal Justice Act, 1994 dated March 2005*.

To this extent, safeguards are in place with the Company's processor and banks to prevent deposits from sanctioned jurisdictions. The Company's employees are aware of the aforementioned policy in order to ensure that no payments are made to any of the aforementioned countries.

10 Approval of Business Introdurers, Affiliates and Business to Business

The Company follows a risk-based approach in its dealings with business associates, including Affiliates and Business Introdurers, while maintaining the exclusive world- wide right, granted to it by its parent company, for the operation of the domain and trading platform on this website.

In overall terms:

- **Affiliates:** Affiliates are generally operators of websites to which the Company (acting direct or through its branch or through any associate acting at the Company's request) grants a non-exclusive, non-transferable, revocable license) to place weblink on their respective websites and b) to use the Company's logo and trade name provided to the Affiliates, for the sole purpose of the Company.
- **Business Introdurers:** are either natural or legal persons who because of their knowledge and standing in a local marketplace have the ability, on a non-exclusive basis, to introduce customers to the Company and the trading platform.

Client to be enabled to trade, the Company undertakes a comprehensive on-boarding process comprising of two constituent elements:

- i. Assessment of appropriateness, with respect to the clients' knowledge and experience.
- ii. AML review, through the completion of KYC and AML procedures. This includes the construction of the client's economic profile, by collecting among other things, information on the client's financial situation and source of funds.

None of the affiliates or business introdurers can have any role or involvement in either the assessment of appropriateness or in the AML review of any client that they introduce or refer to the Company. **The Company has the full and sole right to decline any business that fails any of the above on boarding requirements.**

In turn, the on boarding process for any Affiliate or Business Introdurer, comprises three constituent elements:

- a) KYC / AML review work (see below) of the Affiliate / Business Introdurer.
- b) reputational assessment and investment services risks analysis (to minimize the risk of any breach of the requirements of MiFID and of any equivalent South African legislation).
- c) Legal and commercial agreement setting out respective duties, responsibilities, rights, and obligations.

10.1 Approval process for Business Introdurers and Affiliates.

FRONTIER MARKETS (PTY) LTD, Registration number 023/780267/07 is a private company incorporated in accordance with the laws of South Africa an authorised Financial Services Provider registered as such in terms of the Financial Advisory and Intermediary Services Act, 2002 under FSP No. 53333
FRONTIER MARKETS Pty Ltd Address 11 WALNUT ROAD, DURBAN CENTRAL, DURBAN, KWA-ZULU NATAL, 4001

With respect to AML / KYC, the following due diligence measures are performed for Business Introducers and Affiliates:

1. Verification of identity - Prior to engaging with any Business Introducer or Affiliate, the Company requests and collects the following documents depending on the nature of the person:
 - a. Natural Person:
 - Proof of ID.
 - Proof of Residence.
 - Clean World Check result.
 - b. Legal Person:
 - Company's full name.
 - Company's Address (place of operations).
 - Certificate of registered address.
 - Certificate of Incorporation.
 - Certificate of Directors and Secretary.
 - Certificate of Shareholders.
 - Proof of residence of all shareholders with more than 10% holdings.
 - Proof of identity of any shareholder with more than 10% holdings.
 - POI and POR of the contact person if other than the shareholders.
 - Trade or brand name used by the Affiliate in offering its services

NOTE: For legal persons incorporated outside the Republic of South Africa, the Company shall request and obtain documents similar to the above.

2. Information on the business activities and profile of the Business Introducer / Affiliate to have an overall understanding of who the Business Introducer/Affiliate is and of its general reputation and conduct. Through our Reputational Risk Assessment, we ensure we deal with Business Introducers and Affiliates of good repute, who are fit and proper and have not been involved in any criminal matters or any incidents of breach of investment services or of other professional conduct standards.
3. Confirmation of the residency of clients – The Company does not accept as clients, residents from several jurisdictions as these are indicated on its website. To this extent, the Company confirms the location/residency of the clients and/or potential clients that the Business Introducer/Affiliate will be introducing to ensure that they will not be introducing or promoting the Company's services in banned jurisdictions.
4. Marketing tools - Identification of marketing methods used by the Business Introducer or Affiliate i.e., online (emails, website advertising) and/or offline (office, meeting potential clients in advance, training prior to introducing them, calling potential clients etc.) and review of the website used (where applicable). As per the Company's agreements with Business Introducers and Affiliates, they are prohibited from promoting the Company's services in Adult or Gambling related websites.
5. Payment methods – The Company ensures that all payments are made to a bank account on the name of the Business Introducer or Affiliate established in a regulated bank in an approved jurisdiction.

10.2 Business to Business (“B2B”) activities and approval process

The Company also engages in business to business (“B2B”) activity by offering liquidity and acting as a hedging counterparty solely to regulated investment firms. The business relationship is based on an Institutional Client Agreement between the Company and the B2B Client. In this Agreement, it is clearly and explicitly stipulated that the Company has no responsibility, legal, regulatory, or otherwise to the underlying clients of the B2B Client. **The Company does not receive or handle funds for or on behalf of the underlying clients of B2B Clients.**

The on boarding process for any B2B Client, comprises of four constituent elements:

- a) KYC/AML review work (see below) of the B2B Client premised on primarily the principles set out in the Wolfsberg Questionnaire, as further described below.
- b) Reputational assessment and investment services risks analysis (to minimize the risk of any breach of the requirements of MiFID and of the equivalent South African legislation).
- c) Credit risk assessment on the B2B Client with a recommendation to the Management Committee on the trading limits and terms.
- d) Legal and commercial agreement setting out respective duties, responsibilities, rights, and obligations.

With respect to AML/KYC, the following due diligence measures are performed for B2B Clients:

1. Collection of License certificate – the Company ensures that the third party is properly licensed to offer its services to its underlying clients.
2. Collection of KYC documentation – the Company collects the following:
 - company’s full name.
 - company’s Address (place of operations).
 - certificate of Incorporation.
 - memorandum of Incorporation.
 - certificate of Registered Address.
 - certificate of Directors and Secretary.
 - certificate of Shareholders.
 - proof of residence of all shareholders with more than 10% holdings.
 - proof of identity of any shareholder with more than 10% holdings.
 - information and economic profile of all shareholders with a beneficial ownership of more than 10%.
 - board resolution for the opening of the trading account indicating the authorised person.
 - POI and POR of the authorised person if other than the shareholders; and
 - latest audited financial statements.

3. Confirmation of the application of AML procedures by the third party - the Company requires the completion of a prescribed AML Questionnaire that has been developed along the principles set out in the Wolfsberg Questionnaire (**Appendix 11**). Subject to the answers provided by the B2B Client – especially around the procedures established for on boarding underlying clients, the AML governance culture, ethos, framework, policies and procedures, and the envisaged relationship, the Company may request supporting documentation and/or further information prior to proceeding with the Institutional Client Trading Agreement.
4. Information on the business activities and profile of the B2B Client to have an overall understanding of the business activities, the financial standing and sources of the B2B Client, the background and profile of the key Directors, management, shareholders, and persons exercising significant influence and of the B2B Client’s general reputation and conduct.
5. Location of the B2B Client – the Company confirms that the third party or the controllers of such B2B Client (as appropriate) do not operate from a country with strategic AML deficiencies in accordance with the FATF guidelines.
6. Good repute search – the Company proceeds with online search of the B2B client’s profile to identify possible issues and alerts. Through our Reputational Risk Assessment, we ensure we deal with B2B Clients of good repute, who are fit and proper and have not been involved in any criminal matters or any incidents of breach of investment services or of other professional conduct standards.
7. Clean World Check result – all potential B2B clients, its directors and shareholders need to have a clean World Check result in order to engage with the Company.

11 REPORTING OBLIGATIONS TO FIC

Types of suspicious transactions which may be used for money laundering and terrorist financing are almost unlimited. A suspicious transaction is often defined as any transaction which is out of the ordinary size and scope of a client’s business, size of transactions and personal activities or with the normal business of the specific account. In general, a suspicious transaction will often be one which is inconsistent with the economic profile constructed for the client.

11.1 Recognition of suspicious transactions

- The Company ensures that it maintains adequate information and knows sufficient information about its clients’ activities in order to promptly recognize that a transaction or series of transactions is/are unusual or suspicious.

- The Company takes reasonable steps to ensure that its employees are able to recognize and report suspicious transactions or activity through the provision of appropriate training and the development of this Policy. Such training is provided via both the day-to-day interaction of employees with the Compliance officers, as well as through training sessions which include all relevant departments.
- If the Company knows or suspects that a transaction relates to money laundering or terrorist financing, it refrains from carrying out the transaction before informing FIC.
- The Company recognizes that if it is impossible to refrain from carrying out the transaction or it is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, the MLRO, will inform FIC immediately afterwards.

Appendix 12 provides a list of events that may infer a suspicious transaction.

11.2 Reporting of suspicious transactions to FIC

- The Company, in cases where there is an attempt of executing transactions which it knows or suspects are related to money laundering or terrorist financing, reports its suspicion through the MLRO to FIC.
- The Company also submits to FIC, the clients who have proceeded with the depositing of cash funds equal or exceeding R25,000.00, or any other cash deposits the MLRO upon review considers suspicious and the said funds are not returned to the client until a decision is made by FIC.
- Reports submitted to FIC are done via the online reporting system of the Combating Unit (goAML system).
- All reports related to serious suspicious transactions in relation to money laundering issues must be prepared and sent by the MLRO to FIC following approval of the Executive Director.

After submitting such a report:

- a. The Company may wish to discontinue operating the account of that particular client, so that to ensure that it is not implicated in any money laundering activity.
- b. The Company cooperates fully with FIC and follows any instructions received from them particularly as regards to whether or not to conclude certain trades with the given client. FIC is empowered to instruct the Company to stop, delay or execute a trade with a client, without this being considered a breach of the contractual relationship between the client and the Company.

In any case, the Company must not disclose to the client that it has reported an issue to FIC (tipping off).

The clients' accounts concerned as well as any other connected accounts are placed under the close monitoring of the MLRO.

12 RECORD KEEPING

The Company's policy towards record keeping and archives is as follows:

- a. In case of a suspicious transaction investigation by FIC, the Company will provide without delay the following:
 1. details of the identity of the account.
 2. the identity of the true/beneficial owners of the account.
 3. the identity of the authorized persons who can operate the account.
 4. details of the volume of funds and the transactions performed through the account.
 5. any connected/related accounts.
 6. in relation to specific transactions: -
 - a. the origin of funds,
 - b. the type and amount of the currency involved in the transaction,

- c. the form in which the funds were placed or withdrawn, for example cash, cheques and wire transfers,
- d. the identity of the person that gave the order for the transaction,
- e. the destination of the funds,
- f. the form of instructions and authorisation that have been given,
- g. The type and identification number of any account involved in the transaction.

All the above records are kept for 5 years from the date of execution of the clients' transactions or the termination of the business relationship with the client, as applicable. The documents/data relevant to on-going investigations by MOKAS are kept until the said authority confirms that the investigations are completed, and the case has been closed.

Further to the above mentioned documents/data, any suspicious activity reports are also recorded.

- b. Documents are kept in electronic form as required in this Policy. Retention of the documents/data may be kept electronically, provided that the Company is able to retrieve the said documents/data without any delay and present them at any time to FSB or to FIC, after request.
- c. Retaining identification documents of the client and evidence of the "world-check" performed.
- d. Retaining details of the transactions of the clients (client statements).
- e. Retaining internal and external reports on suspicious transactions which were actually reported.
- f. Retaining annual reports of the MLRO.
- g. Retaining reports on suspicious transactions which were investigated internally but not reported to FIC.
- h. Retaining the signed Monthly Prevention Statements which the company produces with the supporting documentation.
- i. Retaining records of monitoring of both clients KYC documents and transactions compared to

the information submitted as part of the economic profile.

13. TRAINING

The training program aims at educating employees on the recognition and handling of transactions and activities which may be related to money laundering or terrorist financing as well as providing an update on the latest developments in this area. The training sessions are structured to ensure relevance to the roles, duties, and responsibilities of the Company's personnel.

Training shall be provided on important legal provisions as well as updates on important legislative amendments and on the system and procedures followed in relation to the matters below:

- Relevant Anti-Money Laundering Legislation which is effective in the Republic of South Africa.
- Directives issued by EU competent authorities in relation to the prevention of the use of the financial system for legalization of proceeds from money laundering and terrorist financing activities.
- Guidance and Circulars issued by FSB and FIC in relation to AML legal framework; and
- Identification and handling of transactions and activities which may relate to money laundering and terrorist financing activity.

Training on issues regarding the prevention of money laundering and terrorist financing should be provided at least once a year to key management and employees in key positions. Training in relation to

changes to any of the above matters should be provided on an ad hoc basis as and when any significant changes take place.

The training program has a different structure for new employees and existing employees and for different departments of the Company according to the services provided. In respect of establishing an AML/KYC culture across the organization, all employees should be trained on the respective issues. All the employees of the Company's holding company are subject to annual online AML training approved by the Company's MLRO. The Company keeps records and/or evidence for the personnel who attended training/seminars and ensures that proper record keeping procedures are established.

Training Plan

It is noted that the MLRO shall prepare a training plan for each year. The training plan shall at least include the following information:

- Summarized data of the program/content of the training courses/seminars including online training and regulatory training.
- Number and duration of the training courses/seminars.
- Instructors' names and qualifications (where applicable).
- Whether the training courses/seminars were performed in-house or by an external organization or consultants.
- Information for the educational material received.

In addition, the MLRO shall have available information on the specific way/method with which the adequacy and effectiveness of staff training has been assessed and reference to the results and receive feedback from the trainees regarding the quality of the course/seminar and the effectiveness of the trainer.

Signature  _____ CEO

APPENDIX 1

INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

A. INFORMER'S DETAILS

Name	Position and Department
Tel (including extension)	Email Address

B. CUSTOMER'S DETAILS

Name:	AID:
Country of residence:	Citizenship:

C. INFORMATION/SUSPICION

Brief description of activities/transactions	
Reason(s) for suspicion:	
Date and Signature:	

FOR MONEY LAUNDERING COMPLIANCE OFFICER'S USE

Date received:	Reference:

APPENDIX 2

INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

Reference: Customer's Details:
Informant: Department:

INQUIRIES UNDERTAKEN (Brief Description)

.....
.....
.....

ATTACHED DOCUMENTS

.....
.....
.....
.....

COMPLIANCE OFFICER 'S DECISION

.....
.....
.....

FILE NUMBER.....

MLRO's SIGNATURE DATE

.....

APPENDIX

3

EU Equivalent Jurisdictions

1. Australia
2. South Korea
3. Brazil
4. Mexico
5. Canada
6. Singapore
7. Hong Kong
8. Switzerland
9. India
10. South Africa
11. Japan
12. The United States of America
13. Netherlands Antilles (as the Dutch overseas territories)
14. Aruba (as the Dutch overseas territories)
15. Jersey (as UK Crown Dependencies)
16. Guernsey (as UK Crown Dependencies)
17. Isle of Man (as UK Crown Dependencies)
18. Mayotte (as French overseas territories)
19. New Caledonia (as French overseas territories)
20. French Polynesia (as French overseas territories)
21. Wallis and Futuna (as French overseas territories)
22. Saint Pierre and Miquelon (as French overseas territories)



APPENDIX 4

HIGH RISK CLIENTS

Type: Politically Exposed Persons (PEPs)

Purpose: Client onboarding/Annual Review [strike through as appropriate]

A. Customer's information

<u>Name</u> :	
<u>Citizenship</u> :	
<u>Date of Birth</u> :	
<u>Address</u> :	
<u>Place of Birth</u> :	
<u>Registration Date</u> :	

B. Checklist of documents/information

Identification documents:	Date Checked	Date Checked	Date Checked	Date Checked
Valid Proof of identity (indicate number):				
Proof of Residence (Utility bill, Bank statement etc.) no more than 6 months old:				

Customer's economic profile	Date Checked	Date Checked	Date Checked	Date Checked
Has the customer answered the question relating to the establishment of his source of wealth and economic profile?				
Do the activities in his account match the information received?				

Enhanced measures:	Date Checked	Date Checked	Date Checked	Date Checked
Has World Check been performed?				

Have we received a reference letter from a reputable third party to assess the business reputation?				
What are the customer's main business/professional activities?				
What is the expected source used for incoming funds credited to the account?				
What is the anticipated turnover?				

C. Comments:

--

D. Management's approval:

Decision:	
Limitations placed on the account:	



APPENDIX 5

Joint Account Application Form

ACCOUNT HOLDER 1

FINANCIAL SECTOR Name and Address:

Surname: Forenames:

Title (Mr./Mrs./Miss/other): Date of Birth:

Permanent Residential Address:

City/Town: Country: Postcode:

Time spent at your current address:

*Provide the previous address if less than 3 years: City/Town:

Country:

Postcode:

CONTACT DETAILS

Telephone: Email:

ACCOUNT HOLDER 2

Surname: Forenames:

Title (Mr./Mrs./Miss/other): Date of Birth:

Permanent Residential Address:

City/Town: Country: Postcode:

Time spent at your current address:

*Provide the previous address if less than 3 years: City/Town:

Country:

Postcode:

CONTACT DETAILS

Telephone: Email:



We hereby confirm that we
[Names in Full]

and ("Joint Account

Holders") are applying to FRONTIER MARKETS (PTY) LTD ("the Company") for a joint trading Account and enclose this Declaration Form for your consideration.

By applying for a Joint Trading Account with the Company we fully understand that if granted:

- The Account will be opened in our joint names.
- The Account will be allocated a single account number.
- The Account will be allocated only one Log-in and Password.
- The above is not a multiple user Log-in and will only support one user at any one time.

By signing this Declaration Form, we BOTH declare to the Company that:

- We will be jointly and severally responsible for the managing of the Account.
- We have read and understood the terms of this Declaration and the Company's Terms and Conditions (policy on 'Joint Accounts').
- The Company can act on the instructions of either of us without having to first obtain confirmation from the other Joint Account holder unless there is a dispute between us, in such circumstances, we must inform the Company of such a dispute. In cases of dispute all of us may be required to provide the Company with written instructions on the management of the account.
- That the information that we have provided in this form is true and correct and we will notify the Company in writing if any information provided changes or ceases to be correct.

Please note that the email address that you specify in this Declaration Form will be used as a main form of communication with you in the future.

Signed on this day the _____ of _____

Name in full ACCOUNT HOLDER 1

Signature _____

Name in full ACCOUNT HOLDER 2

Signature _____



SUPPORTING DOCUMENTS

**Please upload your documents (including this form) to our website via the My Account section,
or send it via mail.**

Mail: support@frontierm.com

APPENDIX 6

Banned jurisdictions

1. Bosnia
2. Herzegovina
3. Uganda
3. Yemen
4. Iran
5. Iraq
6. Syria
7. Afghanistan
8. North Korea
9. Laos



APPENDIX 7

Client identification checklists for specific client types

SUMMARY OF REGULATIONS 3 – 16 TO FINANCIAL INTELLIGENCE CENTRE ACT ESTABLISHING AND VERIFICATION OF IDENTITY

Natural Persons

Natural person who is a South African citizen or resident in South Africa (Regulations 3 & 4) **Part A**

Natural person who is a citizen of another country and not resident in the Republic (Regulations 5 & 6) **Part B**

South African Company¹ **Part C1**
(Regulations 7 & 8)

Close Corporation² **Part C2**

Foreign Company³ **Part D**
(Regulations 9 & 10)

Legal person other than a Company, Close Corporation or Foreign Company **Part E**
(Regulations 11 & 12)

Partnership **Part F**
(Regulations 13 & 14)

Trust⁴ **Part G**
(Regulations 15 & 16)

¹ A company as defined in Section 1 of the Companies Act, 1973, (Act No. 61 of 1973)

² A corporation as defined in Section 1 of the Close Corporations Act 1984 (Act No. 69 of 1984)

³ An association of natural or legal persons incorporated outside the Republic which has legal personality or enjoys a similar status in terms of which it may enter into contractual relations and legal proceedings in its own name

⁴ A trust as defined in Section 1 of the Trust Property Control Act, 1988 (Act No. 57 of 1988), other than a trust established by virtue of a testamentary writing; by virtue of a court order; in respect of persons under curatorship, or by the trustees of a retirement fund in respect of benefits payable to the beneficiaries of that retirement fund, and includes a similar arrangement established outside the Republic

PART A

ESTABLISHMENT AND VERIFICATION OF IDENTITY OF A NATURAL PERSON WHO IS A CITIZEN OF OR A RESIDENT IN THE REPUBLIC

INFORMATION TO BE OBTAINED	METHOD OF VERIFICATION
Full names Date of birth Identity number	Identification document ⁵ of the person, or document bearing photograph of the person, his or her full names or initials and surname, date of birth and identity number ⁶ , and information obtained from any other independent source ⁷ .
Income tax registration number (if issued)	Document issued by South African Revenue Services bearing number and name of the natural person.
Residential address	Information which can reasonably be expected to achieve verification and is obtained by reasonably practical means ⁸ .
If the Company is aware or ought reasonably to be aware that the person does not have the legal capacity to establish a business relationship or conclude a single transaction without the assistance of another person, the Company must, in addition to obtaining the above particulars, obtain from, or in respect of that other person, his or her:	
Full names Date of birth Identity number	Identification document ⁹ of the person, or document bearing photograph of the person, his or her full names or initials and surname, date of birth and identity number ¹⁰ , and information obtained from any other independent source ¹¹
Residential address	Information which can reasonably be expected to achieve verification and is obtained by reasonably practical means ¹²
Contact particulars	Not necessary to verify

⁵ "Identification document" means an official identity document

⁶ Only in the case where the person is, for a reason that is acceptable to the institution, unable to produce an identification document then the person may produce another document issued to that person, which, considering any guidance notes concerning the verification of identities which may apply to the institution, is acceptable to the institution and contains the information stated

⁷ If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution.

⁸ Considering any guidance notes concerning the verification of identities which may apply to the institution.

⁹ "Identification document" means an official identity document

¹⁰ Only in the case where the person is, for a reason that is acceptable to the institution, unable to produce an identification document then the person may produce another document issued to that person, which, considering any guidance notes concerning the verification of identities which may apply to that institution, is acceptable to the institution and contains the information stated

¹¹ If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution.

¹² Considering any guidance notes concerning the verification of identities which may apply to the institution

Proof of authority to act	Any document evidencing the other person's authority to act on behalf of the person establishing a relationship with the Company, such as a mandate, or letter appointing such person as executor, curator, guardian, as the case may be.

PART B

ESTABLISHMENT AND VERIFICATION OF IDENTITY OF A FOREIGN NATURAL PERSON

INFORMATION TO BE OBTAINED	METHOD OF VERIFICATION
Full names Date of birth Nationality Passport number	Passport; and identification document ¹³ of the person; and information obtained from any other independent source ¹⁴ .
South African income tax registration number (if issued)	Document issued by South African Revenue Services bearing such a number; and Information obtained from any other independent source (see footnote 14)]
Residential address	Not to be verified
If the Company is aware or ought reasonably to be aware that the person does not have the legal capacity to establish a business relationship or conclude a single transaction without the assistance of another person, the Company must, in addition to obtaining the above particulars, obtain from, or in respect of, that other person, his or her:	
Full names Date of birth Nationality Passport number	Identification document ¹⁵ of the person; and Information obtained from any other independent source ¹⁶
Residential address Contact particulars Proof of authority to act	Not to verify Any document evidencing the other person's authority to act on behalf of the person establishing a relationship with the Fund, such as a mandate, or letter appointing such person as executor, curator, guardian, as the case may be.

¹³ "Identification document" means a passport issued by the country of which the person is a citizen

¹⁴ If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

¹⁵ "Identification document" means a passport issued by the country of which the person is a citizen

¹⁶ If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

PART C1

ESTABLISHMENT AND VERIFICATION OF IDENTITY OF A SOUTH AFRICAN FUND

INFORMATION TO BE OBTAINED	METHOD OF VERIFICATION
<p><u>In respect of Fund itself:</u></p> <p>Registered name Registration number under which it is incorporated Registered address</p>	<p>The most recent versions of:</p> <p>Certificate of Incorporation (CM1) and Notice of Registered Office and Postal Address (CM22), both bearing the stamp of the Registrar of Companies and signed by fund secretary.</p> <p>information obtained from any other independent source¹⁷;</p>
<p>Name under which it conducts business</p> <p>Address from which it operates, or if it operates from multiple addresses:</p> <p>a. the address of the office seeking to establish a business relationship or to enter into a single transaction with the Fund; and</p> <p>b. the address of its head office</p>	<p>information which can reasonably be expected to achieve verification and is obtained by reasonably practical means¹⁸;</p> <p>and</p> <p>Information obtained from any other independent source (see footnote 17)</p>
<p>Income tax and value added tax registration numbers of the Fund (if issued)</p>	<p>Document issued by South African Revenue Services bearing numbers AND</p> <p>Information obtained from any other independent source (see footnote 17)</p>
<p><u>In respect of the manager¹⁹ of the fund and each natural person who purports to be authorised to establish a business relationship or conclude a transaction on behalf of fund with the Company: -</u></p>	

¹⁷If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

¹⁸ Considering any guidance notes concerning the verification of identities which may apply to the institution

¹⁹ Manager means the natural person who is the principal executive officer of the fund, by whatever name he or she may be designated and whether or not he or she is a director of the Fund

<u>If a citizen of or resident in the Republic:</u> Full names Date of birth Identity number	Apply verification methods set out in PART A and Information obtained from any other independent source ²⁰
Residential address Contact particulars	Not to be verified
<u>If a foreign national: -</u> Full names Date of birth Nationality	Apply verification methods set out in PART B and information obtained from any other independent source (see footnote 21)
Residential address Contact particulars	Not to be verified
<u>in respect of each person/entity holding 25% or more of the voting rights at a general meeting of the fund: -</u>	
<u>If a citizen of or resident in the Republic:</u> Full names Date of birth Identity number	Apply verification methods set out in PART A and Information obtained from any other independent source ²¹
Residential address Contact particulars	Not to be verified
<u>If a foreign national:</u> Full names Date of birth Nationality	Apply verification methods set out in PART B and Information obtained from any other independent source (see footnote 21)
Residential address Contact particulars	Not to be verified

²⁰ If it is believed to be reasonably necessary considering any guidance notes concerning the verification of identities which may apply to the institution

²¹ If it is believed to be reasonably necessary considering any guidance notes concerning the verification of identities which may apply to the institution

<u>In respect of each person/entity holding 25% or more of the voting rights at a general meeting of the Fund (continued): -</u>	
<p><u>If a South African Fund or close corporation: -</u></p> <p>Registered name Registration number under which it is incorporated Registered address Name under which it conducts business Address from which it operates; or if it operates from multiple addresses: -</p> <p>a. the address of the office seeking to establish a business relationship or to enter into a single transaction with the Company; and</p> <p>b. the address of its head office.</p>	<p>Apply verification methods set out in PART C1 or C2 (as applicable); and</p> <p>Information obtained from any other independent source²²</p>
<p>Residential address Contact particulars</p>	<p>Not to be verified</p>
<p><u>If a foreign fund:</u> The name under which it is incorporated The number under which it is incorporated The address where it is situated for purposes of its incorporation</p>	<p>Apply verification methods set out in PART D; and</p> <p>Information obtained from any other independent source (see footnote 22)</p>
<p>Residential address Contact particulars</p>	<p>Not to be verified</p>
<p><u>If legal person other than as referred to above:</u></p> <p>The name of the legal person The address from which it operates Its legal form</p>	<p>Apply verification methods set out in PART E; and</p> <p>Information obtained from any other independent source²³</p>
<p>Residential address Contact particulars</p>	<p>Not to be verified</p>
<p><u>If a partnership:</u> Name of partnership</p>	<p>Apply verification methods set out in PART F and</p> <p>Information obtained from any other independent source (see footnote 23)</p>

²² If it is believed to be reasonably necessary, considering any guidance notes concerning the verification of identities which may apply to the institution

²³ If it is believed to be reasonably necessary, considering any guidance notes concerning the verification of identities which may apply to the institution

Residential address Contact particulars	Not to be verified
<u>If a trust:</u> Name of trust Number of trusts	Apply verification methods set out in PART G and [Information obtained from any other independent source (see footnote 23)]
Residential address Contact particulars	Not to be verified

PART C2
ESTABLISHMENT AND VERIFICATION OF IDENTITY OF CLOSE CORPORATIONS

<u>INFORMATION TO BE OBTAINED</u>	<u>METHOD OF VERIFICATION</u>
<p><u>In respect of close corporation itself:</u></p> <p>Registered name Registration number under which it is incorporated Registered address</p>	<p>The most recent versions of:</p> <p>Founding Statement and Certificate of Incorporation (CK1) and Amended Founding Statement (CK2) (if applicable), both bearing the stamp of the Registrar of Companies and signed by an authorized member or employee of close corporation; and</p> <p>Information obtained from any other independent source²⁴</p>
<p>Name under which it conducts business</p> <p>Address from which it operates; or if it operates from multiple addresses:</p> <p>a. the address of the office seeking to establish a business relationship or to enter into a single transaction with Company; and</p> <p>b. the address of its head office</p>	<p>Information which can reasonably be expected to achieve verification and is obtained by reasonably practical means²⁵ and</p> <p>Information obtained from any other independent source (see footnote 24)</p>
<p>Income tax and value added tax registration numbers of the fund (if issued)</p>	<p>Document issued by South African Revenue Services bearing numbers; and</p> <p>Information obtained from any other independent source (see footnote 24)</p>
<p><u>In respect of each member of the close corporation and each natural person who purports to be authorised to establish a business relationship or conclude a transaction on behalf of the close corporation with the Company: -</u></p>	
<p><u>If a citizen of or resident in the Republic: -</u></p> <p>Full names Date of birth Identity number</p>	<p>Apply verification methods set out in PART A and</p> <p>Information obtained from any other independent source²⁶</p>
<p>Residential address Contact particulars</p>	<p>Not to be verified</p>

²⁴If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

²⁵ Taking into account any guidance notes concerning the verification of identities which may apply to the institution

²⁶If it is believed to be reasonably necessary, considering any guidance notes concerning the verification of identities which may apply to the institution

<p><u>If a foreign national:</u> - Full names Date of birth Nationality</p>	<p>Apply verification methods set out in PART B AND [Information obtained from any other independent source (see footnote 26)]</p>
<p>Residential address Contact particulars</p>	<p>Not to be verified</p>

PART D

ESTABLISHMENT AND VERIFICATION OF THE IDENTITY OF LEGAL PERSON OTHER THAN A FUND, CLOSE CORPORATION OR FOREIGN FUND

INFORMATION TO BE OBTAINED	METHOD OF VERIFICATION
<u>In respect of legal person:</u> -	
The name of the legal person The address from which it operates Its legal form	Constitution or other founding document in terms of which legal person created; and Information which can reasonably be expected to achieve verification and is obtained by reasonably practical means ²⁷
Income tax and value added tax registration numbers (if issued)	Document issued by South African Revenue Service bearing such number
<u>In respect of each natural person who purports to be authorised to establish a business relationship or conclude a transaction on behalf of the legal person with the accountable institution:</u>	
<u>If a citizen of or resident in the Republic:</u> Full names Date of birth Identity number	Apply verification methods set out in PART A and information obtained from any other independent source ²⁸
Residential address Contact particulars	Not to be verified

²⁷Taking into account any guidance notes concerning the verification of identities which may apply to the institution

²⁸If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

PART D (Continued)

INFORMATION TO BE OBTAINED

METHOD OF VERIFICATION

<p><u>If a foreign national:</u> Full names Date of birth Nationality</p>	<p>Apply verification methods set out in PART B and Information obtained from any other independent source²⁹</p>
<p>Residential address Contact particulars</p>	<p>Not to be verified</p>

²⁹ If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

PART E

ESTABLISHMENT AND VERIFICATION OF IDENTITY OF PARTNERSHIP³⁰

INFORMATION TO BE OBTAINED

METHOD OF VERIFICATION

<u>In respect of the partnership: -</u>	
The name of the partnership	The partnership agreement in terms of which the partnership was formed
<u>In respect of every partner³¹ and the person who exercises executive control over the partnership and each natural person who purports to be authorised to establish a business relationship or enter into a transaction on behalf of partnership:</u>	
<u>If a citizen of or resident in the Republic:</u> Full names Date of birth Identity number	Apply verification methods set out in PART A; and Information obtained from any other independent source ³²
<u>If a foreign national: -</u> Full names Date of birth Nationality	Apply verification methods set out in PART B and information obtained from any other independent source (see footnote 38)
<u>In respect of every partner³³ and the person who exercises executive control over the partnership and each natural person who purports to be authorised to establish a business relationship or enter into a transaction on behalf of partnership (continued): -</u> <u>In respect of every partner³⁴ and the person who exercises executive control over the partnership and each natural person who purports to be authorised to establish a business relationship or enter into a transaction on behalf of partnership (continued): -</u>	

³⁰These requirements pertain to all partnerships other than a partnership formed by qualified persons to carry on a profession and designated by notice in the Gazette by virtue of section 30(2) of the Companies Act, 1973 (Act no 61 of 1973)

³¹Including every member of a partnership *en commandite*, an anonymous partnership or any similar partnership

³²If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

³³Including every member of a partnership *en commandite*, an anonymous partnership or any similar partnership

³⁴Including every member of a partnership *en commandite*, an anonymous partnership or any similar partnership

<p><u>If a South African Fund or close corporation:</u> -</p> <p>Registered name Registration number under which it is incorporated Registered address Name under which it conducts business Address from which it operates; or if it operates from multiple addresses the: -</p> <p>a. the address of the office seeking to establish a business relationship or to enter into a single transaction with the accountable institution; and</p> <p>b. the address of its head office</p>	<p>Apply verification methods set out in PART C1 or C2 (as applicable) and</p> <p>information obtained from any other independent source³⁵</p>
<p><u>If a foreign Fund:</u> -</p> <p>The name under which it is incorporated The number under which it is incorporated The address where it is situated for purposes of its incorporation</p>	<p>Apply verification methods set out in PART D and</p> <p>Information obtained from any other independent source (see footnote 40)</p>
<p><u>In respect of every partner³⁶ and the person who exercises executive control over the partnership and each natural person who purports to be authorised to establish a business relationship or enter into a transaction on behalf of partnership (continued):</u> -</p>	
<p><u>If legal person other than as referred to above:</u> -</p> <p>The name of the legal person The address from which it operates Its legal form</p>	<p>Apply verification methods set out in PART E and</p> <p>Information obtained from any other independent source³⁷</p>
<p><u>If a trust:</u> -</p> <p>Name of trust Number of trusts</p>	<p>Apply verification methods set out in PART G and</p> <p>Information obtained from any other independent source (see footnote 42)</p>

³⁵If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

³⁶Including every member of a partnership *en commandite*, an anonymous partnership or any similar partnership

³⁷If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

PART F
ESTABLISHMENT AND VERIFICATION OF IDENTITY OF TRUST

INFORMATION TO BE OBTAINED	METHOD OF VERIFICATION
<p><u>In respect of trust itself:</u> -</p> <p>Identifying name and IT number</p>	<p>Trust deed or other founding document in terms of which the trust is created, and</p> <p>In the case of a trust: -</p> <p>(i) created in the Republic, the authorisation given by the Master of the High Court in terms of section 7 of the Trust Property Control Act, 1988 to each trustee of the trust to act in that capacity</p> <p>(ii) created outside the Republic, an official document which reflects these particulars, issued by an authority in the country where the trust is created which administers or overseas laws relating to trusts in that country</p>
<p>Address of Master of High Court where trust registered (if applicable)</p>	<p>The authorisation given by the Master of the High Court in terms of section 7 of the Trust Property Control Act, 1988 to each trustee of the trust to act in that capacity</p>
<p>Income tax registration number of trust (if issued)</p>	<p>Document issued by the South African Revenue Service bearing such number</p>
<p><u>In respect of each trustee, each natural person who purports to be authorised to establish a business relationship or enter into a transaction on behalf of trust AND each founder of the trust:</u> -</p>	
<p><u>If a citizen of or resident in the Republic:</u> -</p> <p>Full names Date of birth Identity number</p>	<p>Apply verification methods set out in PART A and</p> <p>Information obtained from any other independent source³⁸</p>
<p>Residential address Contact particulars</p>	<p>Not to be verified</p>

³⁸If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

<p><u>If a foreign national:</u> -</p> <p>Full names Date of birth Nationality</p>	<p>Apply verification methods set out in PART B and</p> <p>information obtained from any other independent source (see footnote 43)</p>
<p>Residential address Contact particulars</p>	<p>Not to be verified</p>
<p><u>In respect of each trustee and each natural person who purports to be authorised to establish a business relationship or enter into a transaction on behalf of trust (continued):</u></p>	
<p><u>If a South African Fund or close corporation:</u></p> <p>Registered name Registration number under which it is incorporated Registered address Name under which it conducts business Address from which it operates; or if it operates from multiple addresses the: -</p> <p>a. the address of the office seeking to establish a business relationship or to enter into a single transaction with the accountable institution; AND</p> <p>b. the address of its head offices</p>	<p>Apply verification methods set out in PART C1 or C2 (as applicable) AND</p> <p>[Information obtained from any other independent source³⁹]</p>
<p>Residential address Contact particulars</p>	<p>Not to be verified</p>
<p><u>If a foreign Fund:</u></p> <p>The name under which it is incorporated The number under which it is incorporated The address where it is situated for purposes of its incorporation</p>	<p>Apply verification methods set out in PART D and</p> <p>Information obtained from any other independent source (see footnote 44)</p>
<p>Residential address Contact particulars</p>	<p>Not to be verified</p>

³⁹If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

PART F (Continued)

INFORMATION TO BE OBTAINED

METHOD OF VERIFICATION

<u>In respect of each trustee and each natural person who purports to be authorised to establish a business relationship or enter into a transaction on behalf of trust (continued):</u>	
-	
<u>If legal person other than as referred to above:</u> The name of the legal person The address from which it operates Its legal form	Apply verification methods set out in PART E and Information obtained from any other independent source ⁴⁰
Residential address Contact particulars	Not to be verified
<u>If a partnership:</u> - Name of partnership	Apply verification methods set out in PART F and [Information obtained from any other independent source (see footnote 45)]
Residential address Contact particulars	Not to be verified

⁴⁰If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

PART F (Continued)

INFORMATION TO BE OBTAINED

METHOD OF VERIFICATION

<u>In respect of each trustee and each natural person who purports to be authorised to establish a business relationship or enter into a transaction on behalf of trust (continued):</u>	
-	
<u>If a trust:</u> - Name of trust Number of trusts	Apply verification methods set out in PART G AND Information obtained from any other independent source ⁴¹

⁴¹ If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

PART F (Continued)

INFORMATION TO BE OBTAINED

METHOD OF VERIFICATION

<u>In respect of each beneficiary of the trust referred to by name in the trust deed or other founding instrument in terms of which the trust is created: -</u>	
<p><u>If a citizen of or resident in the Republic:</u></p> <p>(i) Full names Date of birth Identity number</p> <p>OR where a beneficiary is not listed by name-</p> <p>(ii) Particulars of how the beneficiaries of the trust are determined</p>	<p>Apply verification methods set out in PART A and</p> <p>Information obtained from any other independent source⁴²</p>
<p>Residential address Contact particulars</p>	<p>Not to be verified</p>
<p><u>If a foreign national: -</u></p> <p>(i) Full names Date of birth Nationality</p> <p>OR</p> <p>(ii) Particulars of how the of the trust are determined</p>	<p>Apply verification methods set out in PART B AND</p> <p>[Information obtained from any other independent source (see footnote 47)]</p>
<p>Residential address Contact particulars</p>	<p>Not to be verified</p>

⁴²If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

PART F (Continued)

INFORMATION TO BE OBTAINED

METHOD OF VERIFICATION

<u>In respect of each beneficiary of the trust referred to by name in the trust deed or other founding instrument in terms of which the trust is created (continued):</u>	
<p><u>If a South African fund or close corporation:</u></p> <p>(i) Registered name</p> <p>Registration number under which it is incorporated</p> <p>Registered address</p> <p>Name under which it conducts business</p> <p>Address from which it operates; or if it operates from multiple addresses the: -</p> <p>a. the address of the office seeking to establish a business relationship or to enter into a single transaction with the accountable institution; and</p> <p>b. the address of its head offices</p> <p>OR</p> <p>(ii) Particulars of how the beneficiaries of the trust are determined</p>	<p>Apply verification methods set out in PART C1 or C2 (as applicable); and</p> <p>Information obtained from any other independent source⁴³</p>
<p>Residential address</p> <p>Contact particulars</p>	<p>Not to be verified</p>

⁴³If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

PART F (Continued)

INFORMATION TO BE OBTAINED	METHOD OF VERIFICATION
<p><u>In respect of each beneficiary of the trust referred to by name in the trust deed or other founding instrument in terms of which the trust is created (continued): -</u></p> <p><u>If a foreign Fund:</u> -</p> <p>(i) The name under which it is incorporated The number under which it is incorporated The address where it is situated for purposes of its incorporation</p> <p>OR</p> <p>(ii) Particulars of how the beneficiaries of the trust are determined</p>	<p>Apply verification methods set out in PART D AND</p> <p>[Information obtained from any other independent source⁴⁴]</p>
<p>Residential address Contact particulars</p>	<p>Not to be verified</p>
<p><u>If legal person other than as referred to above:</u> -</p> <p>(i) The name of the legal person The address from which it operates Its legal form</p> <p>OR</p> <p>(ii) Particulars of how the beneficiaries of the trust are determined</p>	<p>Apply verification methods set out in PART E AND</p> <p>[Information obtained from any other independent source (see footnote 49)]</p>
<p>Residential address Contact particulars</p>	<p>Not to be verified</p>

⁴⁴ If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

PART F (Continued)

INFORMATION TO BE OBTAINED	METHOD OF VERIFICATION
<p><u>In respect of each beneficiary of the trust referred to by name in the trust deed or other founding instrument in terms of which the trust is created (continued): -</u></p> <p><u>If a partnership:</u> -</p> <p>(i) Name of partnership</p> <p>OR</p> <p>(ii) Particulars of how the beneficiaries of the trust are determined</p>	<p>Apply verification methods set out in PART F and</p> <p>[Information obtained from any other independent source⁴⁵]</p>
<p>Residential address</p> <p>Contact particulars</p>	<p>Not to be verified</p>
<p><u>If a trust:</u> -</p> <p>(i) Name of trust Number of trusts</p> <p>OR</p> <p>(ii) Particulars of how the beneficiaries of the trust are determined</p>	<p>Apply verification methods set out in PART G and</p> <p>[Information obtained from any other independent source (see footnote 50)]</p>

⁴⁵ If it is believed to be reasonably necessary considering, any guidance notes concerning the verification of identities which may apply to the institution

APPENDIX 8

Joint Bank Account Declaration Form

Declaration for use of Joint Bank Account

[date / moth / year]

Dear Sirs,

I understand that _____ (**Your Client**) has opened a trading account with FRONTIER MARKETS (PTY) LTD (**the Company**) and has funded or intends to fund this trading account from a joint bank account that he/she holds with me.

I am the _____ (State the relationship) of Your Client.

I hereby declare to you that:

- a) I am fully aware and consent to the use of the joint bank account by Your Client for funding his/her trading account with the Company.
- b) I am fully aware of the purposes of the trading account of Your Client with the Company, including that this may be used for investing in complex financial instruments or speculative trading which carry risk of loss of all capital invested.
- c) I will at all times recognise all actions taken by Your Client with respect to funding the trading account with the Company from our joint bank account, including instructions given for the return of funds available on the trading account maintained at .the Company (including of any profits or losses).
- d) I am not a client of the Company and recognise that the Company does not owe any duties or obligations towards me.
- e) I am solely responsible for advising the Company for any changes in the status of the joint bank account that I maintain with Your Client.
- f) I am fully aware that this Declaration is not subject to any time expiry unless I specifically inform you otherwise and you acknowledge receipt of such advice.

Sincerely,

Name of Joint Account

Holder

Signature

APPENDIX 9

DECLARATION OF CASH DEPOSITS

Please duly complete the information requested below. This is to enable you to comply with the regulatory requirements FRONTIER MARKETS (PTY) LTD is subjected to and particularly with its obligations for taking measures to combat money laundering and terrorist financing. All disclosures are fully confidential in accordance with our Privacy Policy.

TRADING ACCOUNT DETAILS

Client's username: _____
Client's trading account number: _____

PERSONAL DATA

Name: _____

Citizenship: _____

Address (as indicated on the provided proof of residence):

Telephone number: _____

Email address: _____

Passport / ID number (delete as appropriate): _____

CASH DEPOSIT'S DETAILS:

Amount of deposit (include currency):

Bank to which the deposit was made: _____

Branch: _____

Full Address of Branch:

Expected origin of further deposits to the account (e.g., cash, wire transfer): _____

Expected origin of withdrawals from the account (your bank details – bank name, branch, address, IBAN/

acc. number, SWIFT and currency): _____

REASON FOR MAKING DEPOSIT IN CASH

VERIFICATION OF SOURCE OF FUNDS

Please choose below as applicable and complete the relevant section:

Please provide the following details:	Please provide one of the following (certified):
What is your annual salary (please indicate amount and currency)	<ol style="list-style-type: none"> 1. Pay slip (or bonus payment) relevant to the cash deposit 2. Signed letter from an employer confirming salary and/or bonus on a letter-headed paper 3. Bank statement indicating receipt of most recent salary from
Did you receive any bonuses this year?	
Please provide your employer's name and address: Name:	

Salary (including Self –Employed) or Savings from Employment Income

Address: _____	employer OR Tax declaration if self employed 4. Any other proof clearly indicating the source of the cash deposit
What is the nature of your employer's business?	

Sale of investments/ liquidation of investment portfolio

Please provide the following details:	Please provide one of the following (certified):
Description of shares/units/deposits:	1. Investment or savings certificates, contract notes or surrender statements 2. Bank statement clearly showing receipt of funds and investment company name 3. Signed letter detailing funds from a regulated account on letter-headed paper 4. Any other proof clearly indicating the source of the cash deposit
Name of the seller:	
How long were these held:	
What was the sale amount?	
When were the funds received?	

Sale of property

Please provide the following details:	Please provide one of the following (certified):
Full address of property sold:	1. Letter detailing property sale signed by a conveyancer or regulated accountant on a letter-headed 2. Copy of sale of contract 3. Any other proof clearly indicating the source of the cash deposit
Date of sale:	
Total sale amount of property sold:	
How long was the property held?	

Inheritance

Please provide the following details:	Please provide one of the following (certified):
Total amount received:	1. Grant of Probate (with a copy of the will) which must include the values of the estate 2. Copy of the will 3. Signed letter from the executor, attorney or estate trustees on letterhead or Bank Statement 4. Any other proof clearly indicating the source of the cash deposit
Date received:	
Name of deceased:	
Solicitor's details:	
Relationship to deceased:	

_____	_____
-------	-------

Company profits/earnings (including dividends)

Please provide the following details:

Please provide one of the following (certified):

Name and Address of company: Name: _____ Address: _____	<ol style="list-style-type: none"> 1. Copy of latest audited company accounts 2. Letter from a regulated accountant giving details on company's profits, nature of activities and turnover 3. Board of Directors' approval 4. Dividend distribution 5. Tax declaration form 6. Any other proof clearly indicating the source of the cash deposit
Nature of Business:	
Amount of annual profits:	
If dividend: a. Date of receipt of dividend: b. Total amount: c. Name of company paying dividend:	
	If funds come from dividends: <ol style="list-style-type: none"> 1. Bank statement clearly showing receipt of funds and name of company paying dividend 2. Letter detailing dividend details signed by a regulated accountant on letter-headed paper

Gift

Please provide the following details:	Please provide one of the following (certified):
Date received:	<ol style="list-style-type: none"> 1. Evidence of the donor's source of wealth as detailed in this table 2. Letter from donor confirming details of gift and acknowledging the source of the donated funds 3. Any other proof clearly indicating the source of the cash deposit
Total amount:	
Relationship with donor:	
Reason for the gift:	
Source of donated funds:	

Retirement income

Please provide the following details:	Please provide one of the following (certified):
Retirement date:	<ol style="list-style-type: none"> 1. Pension fund statement 2. Letter from regulated accountant 3. Letter from annuity provider 4. Bank statement showing receipt of latest pension income and name of provider 5. Savings account statement indicating payment of income 6. Any other proof clearly indicating the source of the cash deposit
Details of previous profession/occupation:	
Details of pension income source:	

Please provide the following details:	Please provide one of the following (certified):
Amount of loan:	<ol style="list-style-type: none"> 1. Loan agreement 2. Recent loan statements

Loan

Purpose of the loan:	3. Any other proof clearly indicating the source of the cash deposit
Name & Address of lender:	
Date of loan:	

Other income sources

Please provide the following details:	Please provide one of the following (certified):
Nature of income:	1. Appropriate supporting documentation 2. Signed letter detailing funds from a regulated accountant
Amount received:	
Date received:	
Received from whom:	

Please include with this declaration the relevant supportive documentation to justify the source of funds as indicated in the applicable section. Please note that you may be requested to submit additional information and/or documentation upon examination of this form and that non-compliance will lead to the non-credit of the deposit.

By signing this form, you acknowledge and declare that all the aforementioned information that you have disclosed are true, complete, and correct and commit to provide any further information as this may be requested.

Client's Full name: _____

Date: _____

Client's Signature: _____

APPENDIX 10

Investigation form for cash deposits

CASH DEPOSITORS

A. CUSTOMER'S INFORMATION

Name (include AID):	
Nationality:	
DoB:	
Address:	
Place of Birth:	
Introduced by (if relevant):	
Brand:	
Account opened on:	
Total deposits:	
Total withdrawals:	
Date form completed:	

B. IS THE CLIENT FULLY COMPLIANT?

STATUS: Compliant/Not Compliant

Checklist of documents:

Valid Passport/ID/Driver's license (indicate number):	
Proof of Residence (Utility bill, Bank statement etc) no more than 6 months old:	
Has World Check been performed?	
Amount of cash deposit:	

C. Enhance due diligence proofs for

cash

Customer's economic profile:

SWIFT/receipt of deposit (must indicate the name of the client and deposited amount)	
Declaration of cash deposits?	
Does the form indicate clearly, the source of funds? If no, have further information been requested?	

Reason for cash deposit?	
--------------------------	--

D. CUSTOMER'S ECONOMIC PROFILE

Customer's economic profile:

Has the customer answered the question relating to the establishment of his economic profile?	
Do the activities in his account match his economic profile?	
What is his main business/professional activities?	
What is the origin of further incoming funds to the account?	

Comments:

Additional information:

- 1.
- 2.

Findings:

Credit the Cash deposit? YES

NO Suspicious activity? YES

NO Return the Cash deposit? YES

NO

Completed Date:

by:

APPENDIX

11

AML Questionnaire

PLEASE VERIFY THE FOLLOWING:

ANTI-MONEY LAUNDERING QUESTIONNAIRE		
Check below "YES" or "NO" as appropriate.		
Please provide additional information where you answer "NO"		
I. General AML Policies, Practices and Procedures	YES	NO
1. Is the AML compliance program approved by the Institution's Board or senior committee?		
2. Does the Institution have a legal and regulatory compliance program that includes a designated compliance officer that is responsible for coordinating and overseeing the AML framework?		
3. Has the Institution developed written policies documenting the processes that they have in place to prevent, defend, and report suspicious transactions?		
4. Does the Institution have an internal auditor or other independent third party to assess the AML policies and practices on a regular basis?		
5. Does the Institution have a policy prohibiting accounts/relationships with shell banks (i.e., banks incorporated in a jurisdiction in which it has no physical presence)?		
6. Does the institution have policies to ensure that they will not conduct transactions with or in behalf of shell banks through any of its accounts or products?		
7. Does the Institution have policies for Politically Exposed Persons (PEPs), their family and close associates?		
8. If the Institution maintain any branches and subsidiaries – does its AML policies and practices apply to all its branches and subsidiaries in the home country and in locations outside of that jurisdiction?		
II. Risk Assessment		
1. Does the Institution have a risk-based assessment of its customer base and their transactions?		
2. Does the institution determines the appropriate level of enhanced due diligence necessary for categories of customers and transactions that the Institution has reason to believe pose a heightened risk of illicit activities?		
III. Know your Customer (KYC), Due Diligence (DD) and Enhanced Due Diligence (EDD)		
1. Has the institution implemented processes for the identification of those customers on whose behalf it maintains or operates accounts or conducts transactions?		
2. Does the Institution require the collection of information regarding customer's business activities?		
3. Does the Institution assess its customers' AML policies and practices?		
4. Does the Institution have processes to review and update customer information relating to high-risk clients?		

5. Does the Institution have procedures to establish a record for each new customer requiring identification documents and KYC information?		
6. Does the Institution complete a risk-based assessment to understand the normal and expected transactions of its customers?		
IV. Reportable Transactions and Prevention and Detection of Transactions with Illegally Obtained Funds		
1. Does the Institution have policies/practices for the identification and reporting of transactions when required?		
2. Does the Institution have procedures to report cash transactions?		
3. Does the Institution screen customers and transactions against lists of person, entities, or countries issues by government/competent authorities?		
4. Does the Institution have policies to reasonably ensure that it only operates with correspondent banks that possess licenses to operate in their countries of origin?		
V. Transactions Monitoring		
1. Does the Institution have a monitoring program for unusual and potentially suspicious activity that covers funds transfers and monetary instruments such as travelers' checks, money orders, etc?		
VI. AML Training		
1. Does the Institution provide AML training to relevant employees that includes? a. Identification and reporting of transactions that must be reported to government authorities. b. Examples of different forms of money laundering involving the Institution's products and services. c. Internal policies to prevent money laundering.		
2. Does the Institution retain records of such training including attendance and training material?		
3. Does the Institution inform employees of changes in AML law and procedures?		
4. Does the Institution employ third parties to carry out some functions of the Institution?		

<u>Institution's Shareholding Structure</u>	
The Institution hereby, confirms and accepts no other ownership other as set forth below	
NAME	ADDRESS

This form was completed by:

Name:
Title:
Signature:
Date:

APPENDIX 12

Examples of suspicious transactions/activities related to money laundering and terrorist financing.

A. MONEY LAUNDERING

1. Transactions with no discernible purpose or are unnecessarily complex.
2. Use of foreign accounts of companies or group of companies with complicated ownership structures which are unjustifiable based on the needs and economic profile of the customer.
3. The transactions or the size of the transactions requested by the customer do not comply with his usual practice and business activity.
4. Large volume of transactions and/or money deposited or credited into, an account when the nature of the customer's business activities would not appear to justify such activity.
5. The business relationship involves only one transaction, or it has a short duration.
6. There is no visible justification for a customer using the services of a particular Financial Organization. For example, the customer is situated far away from the particular Financial Organization and in a place where he could be provided services by another Financial Organization.
7. There are frequent transactions in the same financial instrument without obvious reason and in conditions that appear unusual (churning).
8. There are frequent small purchases of a particular financial instrument by a customer who settles in cash, and then the total number of the financial instrument is sold in one transaction with settlement in cash or with the proceeds being transferred, with the customer's instructions, in an account other than his usual account.
9. Any transaction the nature, size or frequency appear to be unusual, e.g., cancellation of an order, particularly after the deposit of the consideration.
10. Transactions which are not in line with the conditions prevailing in the market, in relation, particularly, with the size of the order and the frequency.
11. The settlement of any transaction but mainly large transactions, in cash.
12. Settlement of the transaction by a third person which is different than the customer which gave the order.
13. Instructions of payment to a third person that does not seem to be related to the instructor.
14. Transfer of funds to and from countries or geographical areas which do not apply, or they apply inadequately FATF's recommendations on money laundering and terrorist financing.
15. A customer is reluctant to provide complete information when establishes a business relationship about the nature and purpose of its business activities, anticipated account activity, prior relationships with Financial Organisations, names of its officers and directors, or information on its business location. The customer usually provides minimum or misleading information that is difficult or expensive for the Financial Organisation to verify.
16. A customer provides unusual or suspicious identification documents that cannot be readily verified.
17. A customer's home/business telephone is disconnected.
18. A customer that makes frequent or large transactions and has no record of past or present employment experience.
19. Difficulties or delays on the submission of the financial statements or other identification documents, of a customer/legal person.
20. A customer who has been introduced by a foreign Financial Organisation, or by a third person whose countries or geographical areas of origin do not apply, or they apply inadequately FATF's recommendations on money laundering and terrorist financing.

21. Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g., student, unemployed, self-employed, etc).
22. The stated occupation of the customer is not commensurate with the level or size of the executed

- transactions.
23. Financial transactions from non-profit or charitable organizations for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
 24. Unexplained inconsistencies arising during the process of identifying and verifying the customer (e.g., previous, or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address, and date of birth etc).
 25. Complex trust or nominee network.
 26. Transactions or company structures established or working with an unneeded commercial way. e.g., companies with bearer shares or bearer financial instruments or use of a postal box.
 27. Use of general nominee documents in a way that restricts the control exercised by the company's board of directors.
 28. Changes in the lifestyle of employees of the Financial Organisation, e.g., luxurious way of life or avoiding being out of office due to holidays.
 29. Changes in the performance and the behavior of the employees of the Financial Organisation.

B. TERRORIST FINANCING

1. Sources and methods

The funding of terrorist organizations is made from both legal and illegal revenue generating activities. Criminal activities generating such proceeds include kidnappings (requiring ransom), extortion (demanding "protection" money), smuggling, thefts, robbery and narcotics trafficking. Legal fund-raising methods used by terrorist groups include:

- i. collection of membership dues and/or subscriptions,
- ii. sale of books and other publications,
- iii. cultural and social events,
- iv. donations,
- v. community solicitations and fund-raising appeals.

Funds obtained from illegal sources are laundered by terrorist groups by the same methods used by criminal groups. These include cash smuggling by couriers or bulk cash shipments, structured deposits to or withdrawals from bank accounts, purchases of financial instruments, wire transfers by using "straw men", false identities, front, and shell companies as well as nominees from among their close family members, friends, and associates.

2. Non-profit organizations

Non-profit and charitable organizations are also used by terrorist groups as a means of raising funds and/or serving as cover for transferring funds in support of terrorist acts. The potential misuse of non-profit and charitable organizations can be made in the following ways:

- i. Establishing a non-profit organization with a specific charitable purpose, but which actually exists only to channel funds to a terrorist organization.
- ii. A non-profit organization with a legitimate humanitarian or charitable purpose is infiltrated by terrorists who divert funds collected for an ostensibly legitimate charitable purpose for the support of a terrorist group.
- iii. The non-profit organization serves as an intermediary or cover for the movement of funds on an international basis.
- iv. The non-profit organization provides administrative support to the terrorist movement.

Unusual characteristics of non-profit organizations indicating that they may be used for an unlawful purpose are the following:

- i. Inconsistencies between the apparent sources and amount of funds raised or moved.
- ii. A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organization
- .
 - ii. A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit
 - iii.
 - iv. Large and unexplained cash transactions by non-profit
 - v.
- v. The absence of contributions from donors located within the country of origin of the non-profit.

APPENDIX 13

OFFENSES RELATING TO PROCEEDS OF UNLAWFUL ACTIVITIES – POCA 1998

Section 4 - Money laundering

Any person who knows or ought reasonably to have known that property is or forms part of the proceeds of unlawful activities and:

- enters into any agreement or engages in any agreement, arrangement, or transactions with anyone about that property, whether such agreement, arrangement or transaction is legally enforceable or not; or
- performs any other act about such property, whether it is performed independently or in concert with any other person.

which has or is likely to have the effect:

- of concealing or disguising the nature, source, location, disposition or movement of the said property or the ownership thereof or any interest which anyone may have in respect thereof; or
- of enabling or assisting any person who has committed or commits an offence, whether in the Republic or elsewhere:
 - o to avoid prosecution; or
 - o to remove or diminish any property acquired directly, or indirectly, because of the commission of an offence.

shall be guilty of an offence.

The elements of this offence are: -

-
- *Mens rea*: The defendant knew or reasonably ought to have known that the property is the proceeds of unlawful activity.
- Physical element: arrangement or transaction - the defendant must have performed action in relation to the property in question, namely, to enter into an agreement, arrangement or transaction concerning the property or performed any other action with the property.
- Purpose: Concealment or avoidance of prosecution or confiscation as a factual matter. The agreement, arrangement, transaction, or other action must have had, or be likely to have, the effect of concealing or disguising the source of the money or its location or ownership, enabling someone to avoid prosecution or to hide the proceeds of an offence.

Section 5 - Assisting another to benefit from proceeds of unlawful activities

Any person who knows or ought reasonably to have known that another person has obtained the proceeds of unlawful activities, and who enters into any agreement with anyone or engages in any agreement or transaction whereby:

- the retention or the control by or on behalf of the said other person of the proceeds of unlawful activities is facilitated; or
- the said proceeds of unlawful activities are used to make funds available to the said other person or to acquire property on his or her behalf or to benefit him or her in any other way shall be guilty of an offence.

Section 6 - Acquisition, possession, or use of proceeds of unlawful activities

Any person who:

- acquires
- uses; or

- has possession of,

property and who knows or ought reasonably to have known (constructive knowledge) that it is or forms part of the proceeds of unlawful activities of another person, shall be guilty of an offence.

There is no need to establish the purpose of such acquisition, use or possession. There are no requirements to secure a conviction for the underlying predicate offence to secure a conviction for the money laundering offences. All that is required is proof that the property must be described with significant accuracy, but no allegation must be made as to the specific offence from which the property is derived. South African law permits the acceptance of direct evidence as well as circumstantial or other indirect evidence, which is almost always relied upon to prove intent. A person can therefore be convicted of a money laundering offence based on the inferences to be drawn from the objective factual circumstances if these are sufficient to prove the ingredients of the charge.

APPENDIX 14

FINANCIAL INTELLIGENCE CENTRE GUIDANCE NOTE 3A

<https://www.fic.gov.za/DownloadContent/RESOURCES/GUIDELINES/130328%20GUIDANCE%20NOTE%203A.pdf>